A Tahiti, le 23 octobre 2014

LA
S. É .CURITÉ
INF O RMATIQUE
A l'usage des non initiés.

Les petits guides LaTeX
Cybersécurité
Ingénierie sociale.

1 Avant-propos

Ce document aura été rédigé un peu dans l'urgence car, s'il y a maintenant bien des années que j'ai pris conscience du danger des attaques d'ingénierie sociale [1] en particulier, j'espérais qu'elles avaient atteint leur paroxysme et que leur nombre baisserait avec l'aide de l'amélioration du niveau de culture informatique de la population.

Or, non seulement le nombre d'attaques n'a pas baissé, mais leur gravité et leur diversité ont littéralement explosé.

C'est pourquoi, en tant que professionnel, j'ai décidé de mettre à la disposition du public quelques compétences basiques dans le domaine du repérage des attaques.

Afin de ne pas perdre de lecteurs en route, je vais tenter d'aller directement à l'essentiel avec exemples à l'appui. Vous verrez que certaines attaques d'ingénierie sociale sont particulièrement ressemblantes et que la qualité des imitations a énormément progressé elle aussi. Ainsi on y trouve beaucoup moins de fautes ou de caractères exotiques. [2]

Les mécanismes des attaques par ingénierie sociale sont souvent très gros, mais les personnes peu habituées à l'outil informatique et peu méfiante à l'égard de cette invention formidable qu'est Internet en sont souvent les premières victimes.

1. J'en donne une définition plus loin dans le texte
2. Jusqu'à une époque récente, on y trouvait souvent des caractères cyrilliques.

Mon rôle de ”spécialiste” est de sensibiliser autant de personnes que possible à la sécurité informatique car je demeure persuadé qu'avec un peu de sens critique et un peu d'observation, on peut éviter 95 % des problèmes de sécurité informatique, si ce n'est plus.

En matière de sécurité informatique le minimum est très facilement à la portée de tous, encore faut–il en être conscient.

Le présent document a été rédigé sous licence ”Creative Common” afin de permettre une large diffusion du document tout en modifications les modifications ou les utilisations commerciales sans mon accord.

Ce document est orienté spécifiquement sur les attaques d'ingénierie sociale. Si vous voulez en savoir plus sur la sécurité informatique en général, la rédaction d'autres documents est en cours sur le même modèle que celui-ci.

2 L'ingénierie sociale

L'ingénierie sociale est un fléau qui se cache sous une belle formule ! Ingénierie sociale, ça résonne bien, c'est presque élégant à entendre. Mais l'expression bien qu'un peu obtuse désigne quelque chose qui l'est beaucoup moins et qui n'est rien de plus qu'une technique de manipulation mentale fort efficace.

Je vais présenter l'analyse de plusieurs messages permettant de comprendre facilement comment fonctionne l'attaque tentée.

Après cela, j'espère que vous ne regarderez plus votre messagerie ou vos comptes de réseaux sociaux de la même manière

Le document que je soumets à votre sagacité ne comporte rien qui puisse faire penser qu'il est confidentiel, secret et il est au contraire à diffuser le plus possible. (Vérifiez les conditions de la licence)

Dans les semaines qui viennent de se passer, une série de publications réalisées par le CLUSIR Tahiti a commencé à être diffusée dans la presse au compte–goutte, mais malheureusement, cela ne suffit pas. Je contribue à ces publications.

L'ordre des rubriques est établie en fonction d'une certaine logique de priorité.

Afin de définir ce qu'est le spam, je commence par sa définition en montrant quelques exemples. Ensuite, je passe immédiatement au phishing (ou hameçonnage), qui est un fléau connaissant actuellement un pic.

Voici ce que Wikipedia dit de l'ingénierie sociale.

```
L'ingénierie sociale (social engineering en anglais) est une
forme d'acquisition déloyale d'information et d'escroquerie,
utilisée en informatique pour obtenir d'autrui, un bien, un
service ou des informations clefs. Cette pratique exploite
les failles humaines et sociales de la structure cible, à
laquelle est lié le système informatique visé. Utilisant ses
connaissances, son charisme, l'imposture ou le culot, l'atta-
quant abuse de la confiance, de l'ignorance ou de la crédulité
des personnes possédant ce qu'il tente d'obtenir.
```

Article complet en cherchant "ingénierie sociale" dans Wikipedia : `http://fr.wikipedia.org/`

L'objet de la convoitise peut être un mot de passe pour une adresse de messagerie ou un compte sur un réseau social, ce peut être également des coordonnées bancaires, de l'argent ou l'obtention d'information qui permettront de faire chanter la victime.

Je vais essentiellement parler d'ingénierie sociale à travers la messagerie électronique, mais ces procédés sont utilisés également dans les réseaux sociaux et le seront probablement d'autres manières que je n'arrive pas encore à imaginer.

Les techniques sont de divers ordre et il faut toutes les connaître en raison de leur gravité en cas de réussite.

- le SPAM
- le phishing, que j'appelle volontier "hameçonnage" car c'est plus joli,
- le SCAM ou arnaque à la nigerianne,
- les pièces jointes contenant des "malwares" et en particulier les "ramsonwares",
- les chaînes,
- Ayant une imagination particulièrement limitée (un peu d'auto–dérision ne fait pas de mal), je n'exclus pas de prolonger cette liste ultérieurement.

Dans chacune des sections, je vais donner des exemples qui sont en fait des copies de messages bien réels.

2.1 Le SPAM

Cette partie va nous permettre de comprendre ce qu'est le spam et ses variantes.

Globablement le spam est un courrier indésirable ou pourriel (office québecois de la langue française)

Dans chacune des sections, je vais donner des exemples qui sont majoritairement des messages réels.

Il existe plusieurs catégories de spam :

- les chaînes parmi lesquelles :
  - Des messages de chaînes colportant des nouvelles parfois totalement fausses ou proposant de remplir une pétition.
  - Des messages indiquant qu'un virus existe et qu'on risque de recevoir un message avec ce virus, etc... c'est ce qu'on appelle un hoax (ou canular en bon français)
  - Chaînes de superstition.
- les publicités pour des produits parfois contrefaits, des médicaments (faux), etc. Attention, la contrefaçon enrichit les organisations criminelles et autres trafiquants.
  - Publicité pour des faux médicaments visant à renforcer la virilité,
  - Publicité pour des solutions pour gagner beaucoup d'argent en ne faisant pas grand chose. (Si c'était possible, ça se saurait !)
  - etc.
- les scams ou arnaque à la nigériane ou Arnaque 4.1.9 (développé dans une autre section)
- le phishing ou hameçonnage, (développé dans une autre section)
- Les spams avec diffusion de malware, tels que par exemple les ramsonware (développé dans une section distincte), ls keyloggers, etc.

Pour identifier un type de SPAM, il faut en avoir déjà vu quelques–uns.

Une majorité des lecteurs en auront déjà reçu plusieurs centaines sans forcément faire très attention, mais je vais vous inciter à la méfiance pour mieux comprendre ce phénomène.

2.1.1 Quelques exemples de spams ci-dessous.

Les exemples ci-dessous vous paraîtront anodins lorsque vous aurez lu les sections suivantes.

GRAND MARABOUT DU BENIN LA TERRE DE VODOUN - Message (Texte brut)

FICHIER MESSAGE

ven. 04/07/2014 10:37

robert durant <durantrobert9@gmail.com>

GRAND MARABOUT DU BENIN LA TERRE DE VODOUN

À undisclosed-recipients:

Je m'appelle didier tradipraticien je peut intervenir dans les domaines suivants : - amour : retour de l'être aimé, maraboutage d'une femme ou d'un homme, mettre fin à un divorce, attirer quelqu'un... - chance : grigri pour avoir plus de chance aux jeux, pour être un peu moins poissard dans la vie... - travail : incantations magiques pour trouver un travail, ne pas se faire virer, rituels pour être augmenté, rituels pour réussir les entretiens d'embauche - business et affaires: grigri à utiliser quand on monte une entreprise, talisman pour mieux négocier les contrats, prières pour faire venir les clients et attirer des partenaires..
N'hésitez pas à me contacté

Adresse EMail: didierdodji7@gmail.com <mailto:didierdodji7@gmail.com>

robert durant

Même les mediums, voyants extramalins piègent les gogos sur Internet.

jeu. 01/01/1970 14:05

Levtiira + Vigara ~ SAALE! - Message (HTML)

Cheap.Levtiira-Vigarra Now <amweefkuliw@supr.com>

Levtiira + Vigara ~ SAALE!

Mediicattions for life

BEST PRICES

Best Products!

Vigara	0.38$
Levtiirra	0.98$
Cilais	1.28$
Vigarra Sublingual	0.96$
Female Vigarra	1.41$

[>> View all]

Beest Sides!

* Lowest priices and best quality on the market!
* F_D_A approved produucts
* Worldwide shipping, you can trrack delivery progress
* All kind of goodss in one place
* Official suppliers
* Discreet parcel
* Giifts and bonuses
* Payment: VISA and AMEXX. Masterrcard is not supported. Sorryy.
* 1-3 daays shippingg for American customerrs __NEW!

[http://nqvdjfn.yqfymedics.ru]

IMPORTANT! If you don't see liinks or can't cliick on it. Pleese press "Unnblock" or "It's not a spaamm" or somethiing liike that button.

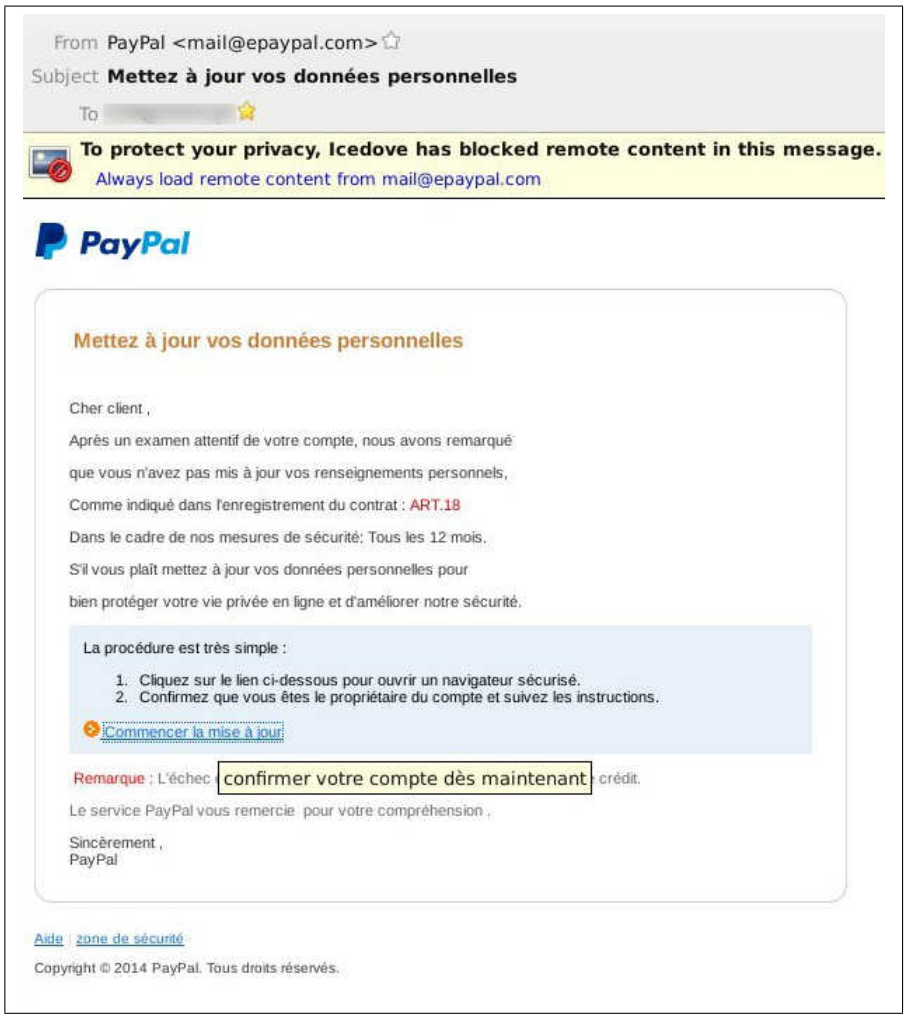
Dopez vos performances avec des contrefaçons qui vous rendront peut-être malades.

D'autres exemples sont présentés et analysés dans les sections suivantes.

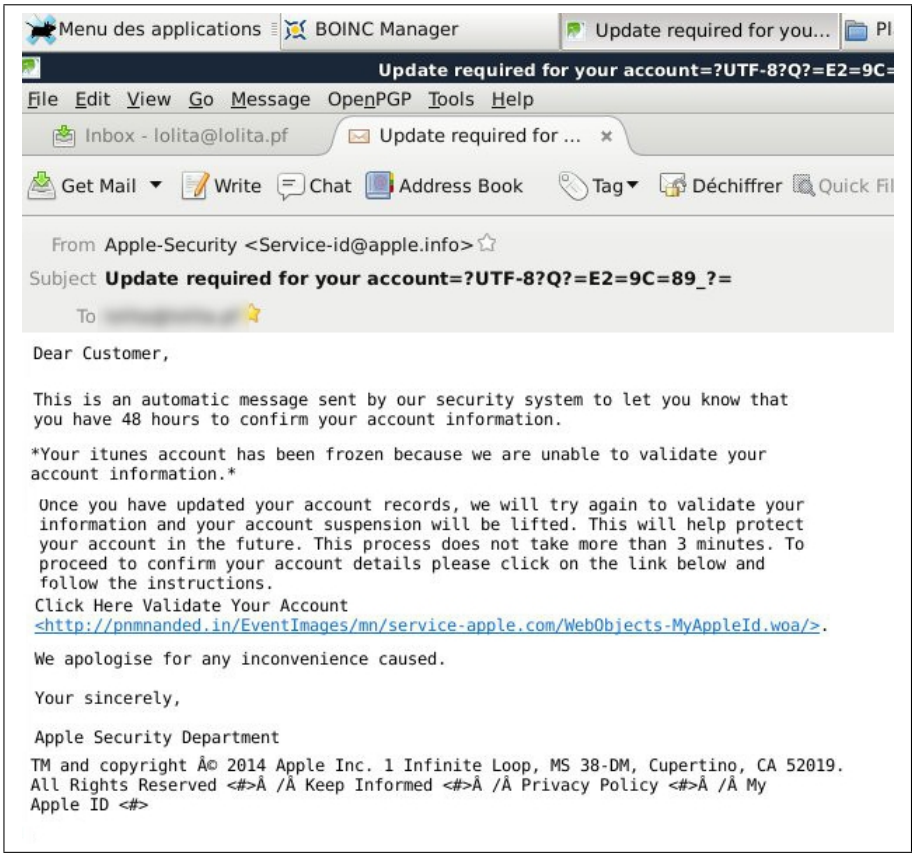
2.2 Analyse d'une série de documents sur le phishing

Les messages ci-dessous sont des exemple de ce que peut être la première attache d'une attaque de phishing.

Avant que vous ne receviez ce message, des gens ont réfléchi, planifié leur coup et préparé un faux site internet, copie presque conforme d'un autre site bien réel.


From PayPal <mail@epaypal.com>
Subject Mettez à jour vos données personnelles
To
To protect your privacy, Icedove has blocked remote content in this message.
Always load remote content from mail@epaypal.com
PayPal
Mettez à jour vos données personnelles
Cher client ,
Après un examen attentif de votre compte, nous avons remarqué
que vous n'avez pas mis à jour vos renseignements personnels,
Comme indiqué dans l'enregistrement du contrat : ART.18
Dans le cadre de nos mesures de sécurité; Tous les 12 mois.
S'il vous plaît mettez à jour vos données personnelles pour
bien protéger votre vie privée en ligne et d'améliorer notre sécurité.
La procédure est très simple :
1. Cliquez sur le lien ci-dessous pour ouvrir un navigateur sécurisé.
2. Confirmez que vous êtes le propriétaire du compte et suivez les instructions.
Commencer la mise à jour
Remarque : L'échec
confirmer votre compte dès maintenant
crédit.
Le service PayPal vous remercie pour votre compréhension .
Sincèrement ,
PayPal
Aide | zone de sécurité
Copyright © 2014 PayPal. Tous droits réservés.

Un faux message Paypal (notez le nom de domaine epaypal.com au lieu de Paypal.com)


Menu des applications
BOINC Manager
Update required for you...
Update required for your account=?UTF-8?Q?=E2=9C=
File Edit View Go Message OpenPGP Tools Help
Inbox - lolita@lolita.pf
Update required for ...
Get Mail
Write
Chat
Address Book
Tag
Déchiffrer
From Apple-Security <Service-id@apple.info>
Subject Update required for your account=?UTF-8?Q?=E2=9C=89_?=
To
Dear Customer,
This is an automatic message sent by our security system to let you know that you have 48 hours to confirm your account information.
Your itunes account has been frozen because we are unable to validate your account information.
Once you have updated your account records, we will try again to validate your information and your account suspension will be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.
Click Here Validate Your Account
<http://pnmnanded.in/EventImages/mn/service-apple.com/WebObjects-MyAppleId.woa/>.
We apologise for any inconvenience caused.
Your sincerely,
Apple Security Department
TM and copyright Â© 2014 Apple Inc. 1 Infinite Loop, MS 38-DM, Cupertino, CA 52019. All Rights Reserved <#>Â /Â Keep Informed <#>Â /Â Privacy Policy <#>Â /Â My Apple ID <#>

Un faux message se présentant comme provenant d'Apple.

Pour analyser et comprendre un document, il faut d'abord l'avoir vu. Il est en anglais, mais ils peuvent arriver dans n'importe quelle langue.

Qu'est-ce que le phishing ou le "hameçonnage" ?

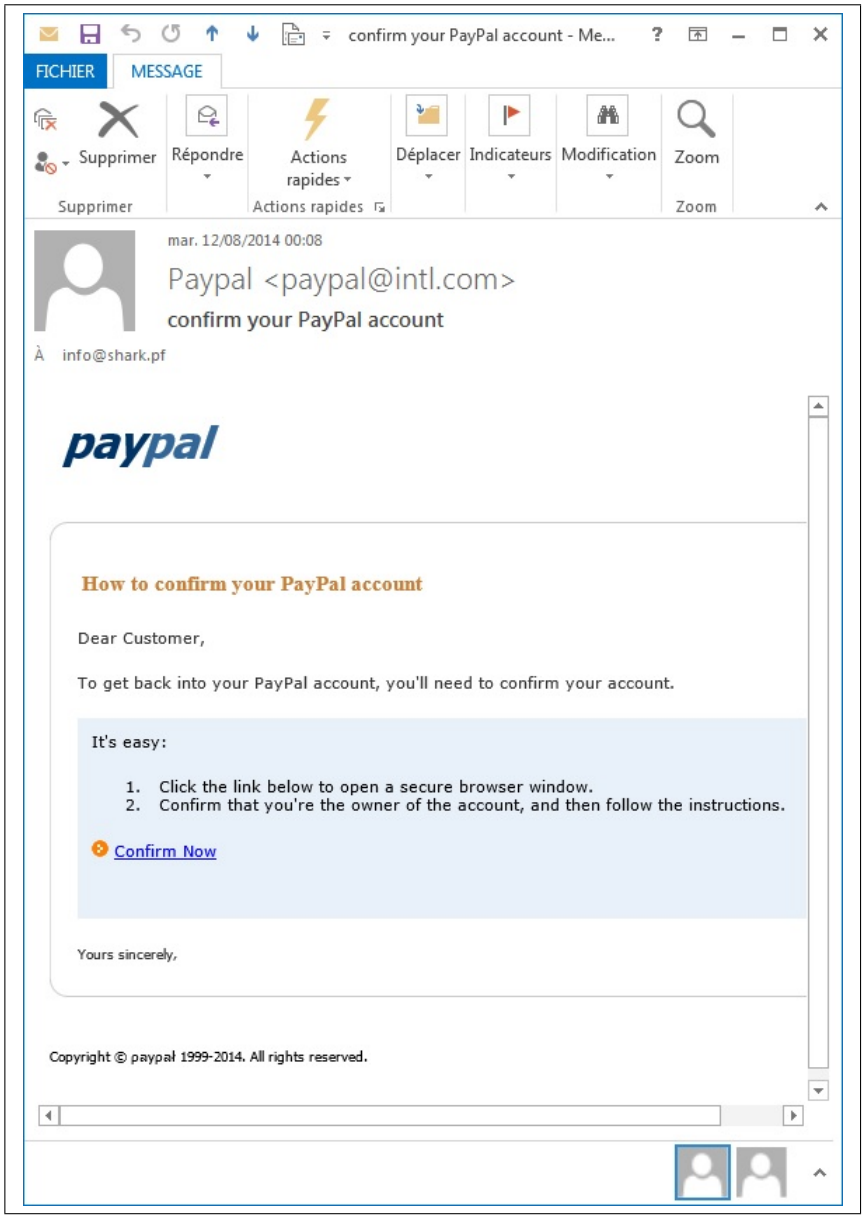
Le phishing, que nos cousins du Québec nomment "hameçonnage" (d'ailleurs tout francophone affirmé devrait en faire autant). Le phishing est dangereux également, il s'apparente au scam et est comme lui, le résultat d'utilisation de techniques de manipulation

Il existe plusieurs catégories de messages de phishing.

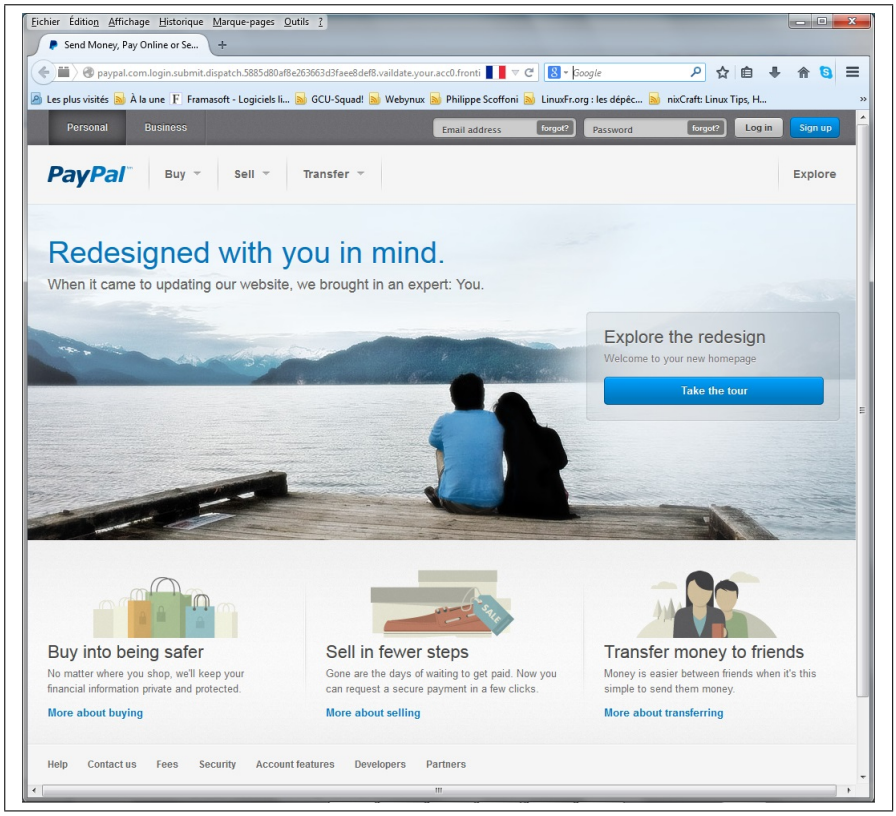
Certains vont directement vous demander de saisir vos informations bancaires sur un site, c'est le premier cas que nous allons étudier.

2.2.1 Vol d'informations bancaires

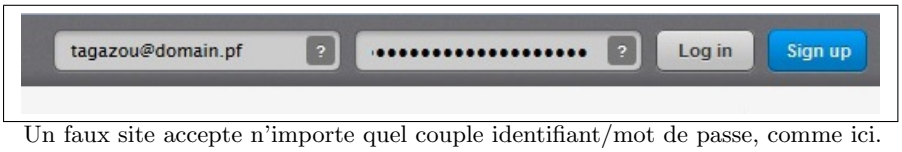
Vol d'informations bancaires - étude de cas n° 1



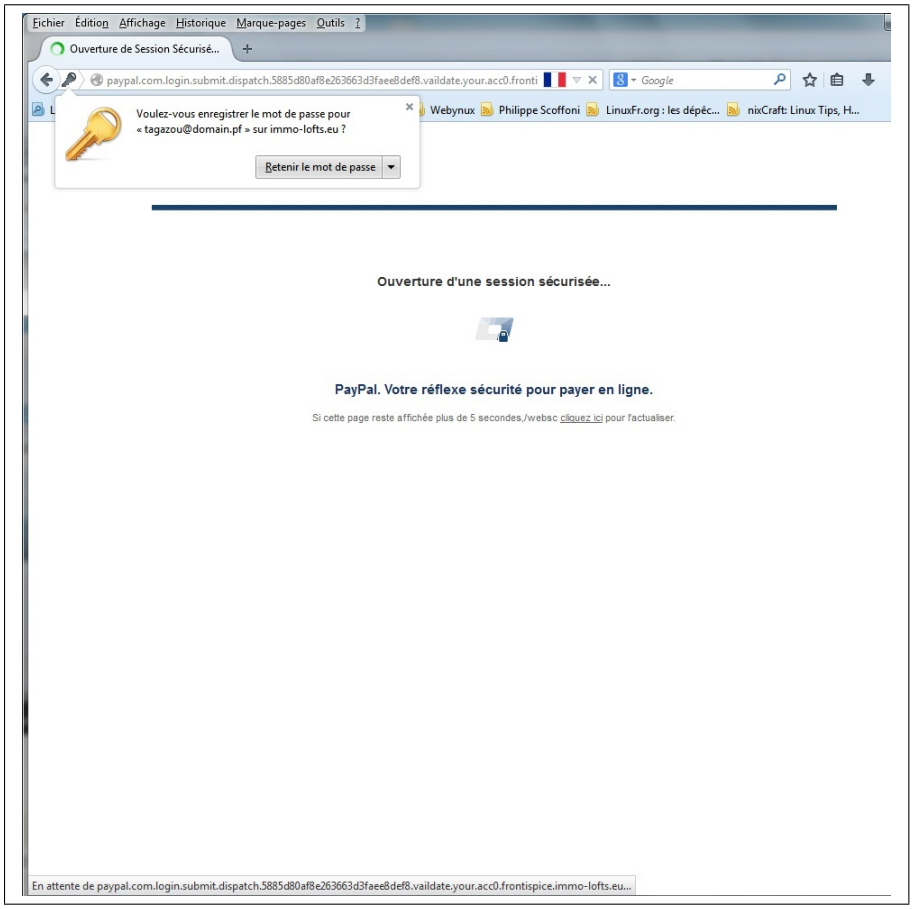
Message initial de l'arnaque


Fichier Édition Affichage Historique Marque-pages Outils ?
Send Money, Pay Online or Se...
paypal.com.login.submit.dispatch.5885d80af8e263663d3faee8def8.vaildate.your.acc0.fronti
Les plus visités À la une Framasoft - Logiciels li... GCU-Squad! Webynux Philippe Scoffoni LinuxFr.org : les dépêc... nixCraft: Linux Tips, H...
Personal Business
Email address forgot? Password forgot? Log in Sign up
PayPal Buy Sell Transfer Explore
Redesigned with you in mind.
When it came to updating our website, we brought in an expert: You.
Explore the redesign
Welcome to your new homepage
Take the tour
Buy into being safer
No matter where you shop, we'll keep your financial information private and protected.
More about buying
Sell in fewer steps
Gone are the days of waiting to get paid. Now you can request a secure payment in a few clicks.
More about selling
Transfer money to friends
Money is easier between friends when it's this simple to send them money.
More about transferring
Help Contact us Fees Security Account features Developers Partners

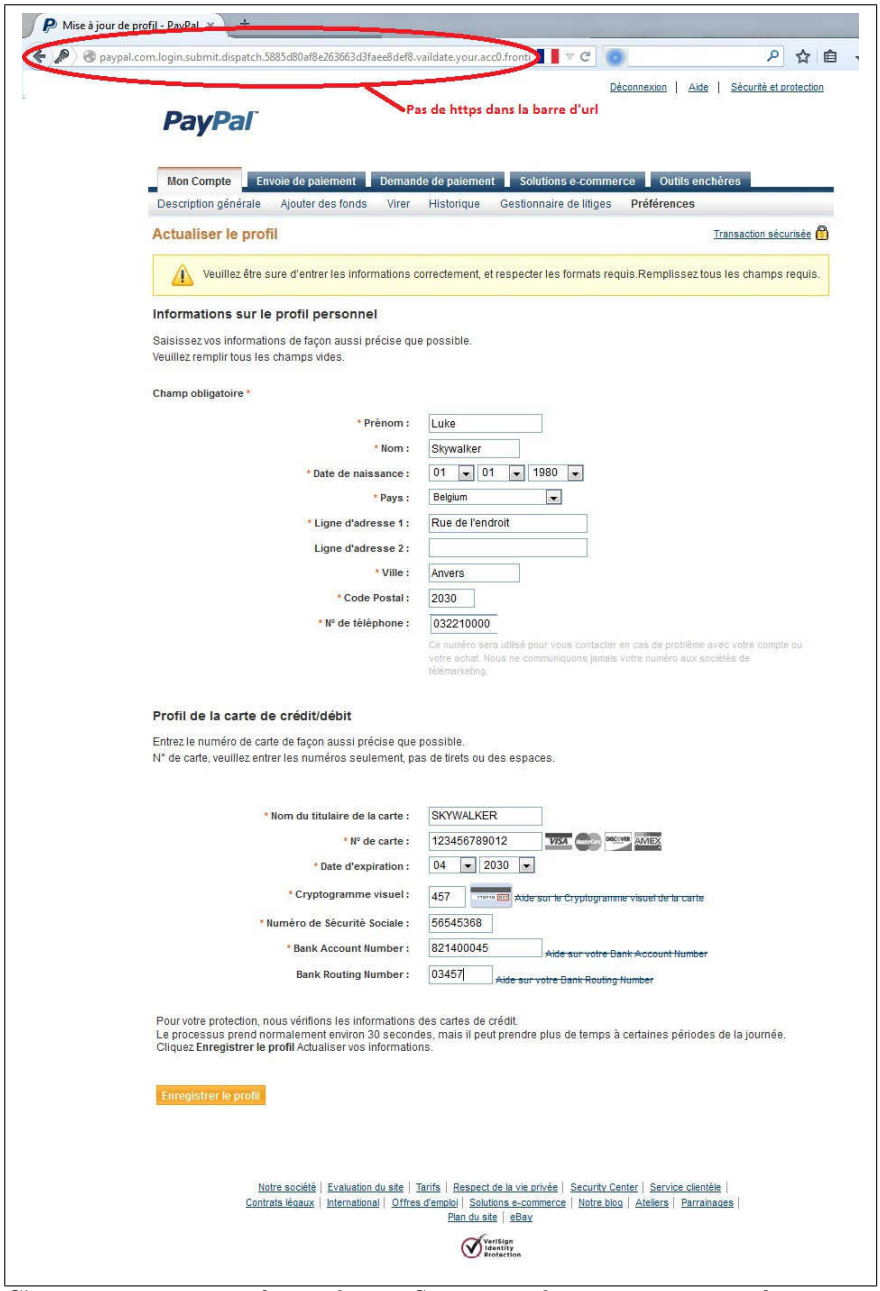
Cette arnaque est très bien faite avec un site très ressemblant



Un faux site accepte n'importe quel couple identifiant/mot de passe, comme ici. Mon identifiant est une adresse courriel fausse tagazou@domaine.pf et j'ai tapé n'importe quoi dans le champs mot de passe.


Fichier Édition Affichage Historique Marque-pages Outils ?
Ouverture de Session Sécurisé...
paypal.com.login.submit.dispatch.5885d80af8e263663d3faee8def8.vaildate.your.acc0.fronti
Google
Webynux
Philippe Scoffoni
LinuxFr.org : les dépêc...
nixCraft: Linux Tips, H...
Voulez-vous enregistrer le mot de passe pour « tagazou@domain.pf » sur immo-lofts.eu ?
Retenir le mot de passe
Ouverture d'une session sécurisée...
PayPal. Votre réflexe sécurité pour payer en ligne.
Si cette page reste affichée plus de 5 secondes,/websc cliquez ici pour l'actualiser.
En attente de paypal.com.login.submit.dispatch.5885d80af8e263663d3faee8def8.vaildate.your.acc0.frontispice.immo-lofts.eu...

C'est vraiment trompeur, mais en réalité cette connexion n'est pas sécurisée comme vous pourrez le voir sur l'image suivante. (pas d'utilisation de https)


Mise à jour de profil - PayPal
paypal.com.login.submit.dispatch.5885d80af8e263663d3faee8def8.vaildate.your.acc0.front
Pas de https dans la barre d'url
Déconnexion | Aide | Sécurité et protection
PayPal
Mon Compte
Envoie de paiement
Demande de paiement
Solutions e-commerce
Outils enchères
Description générale
Ajouter des fonds
Virer
Historique
Gestionnaire de litiges
Préférences
Actualiser le profil
Transaction sécurisée
Veuillez être sure d'entrer les informations correctement, et respecter les formats requis.Remplissez tous les champs requis.
Informations sur le profil personnel
Saisissez vos informations de façon aussi précise que possible.
Veuillez remplir tous les champs vides.
Champ obligatoire *
* Prénom : Luke
* Nom : Skywalker
* Date de naissance : 01 01 1980
* Pays : Belgium
* Ligne d'adresse 1 : Rue de l'endroit
Ligne d'adresse 2 :
* Ville : Anvers
* Code Postal : 2030
* N° de téléphone : 032210000
Profil de la carte de crédit/débit
Entrez le numéro de carte de façon aussi précise que possible.
N° de carte, veuillez entrer les numéros seulement, pas de tirets ou des espaces.
* Nom du titulaire de la carte : SKYWALKER
* N° de carte : 123456789012
* Date d'expiration : 04 2030
* Cryptogramme visuel : 457
Aide sur le Cryptogramme visuel de la carte
* Numéro de Sécurité Sociale : 56545368
* Bank Account Number : 821400045
Aide sur votre Bank Account Number
Bank Routing Number : 03457
Aide sur votre Bank Routing Number
Pour votre protection, nous vérifions les informations des cartes de crédit.
Le processus prend normalement environ 30 secondes, mais il peut prendre plus de temps à certaines périodes de la journée.
Cliquez Enregistrer le profil Actualiser vos informations.
Enregistrer le profil
Notre société | Evaluation du site | Tarifs | Respect de la vie privée | Security Center | Service clientèle |
Contrats légaux | International | Offres d'emploi | Solutions e-commerce | Notre blog | Ateliers | Parrainages |
Plan du site | eBay

C'est ici que vous vous faites plumer. Surtout ne donnez jamais vos informations.

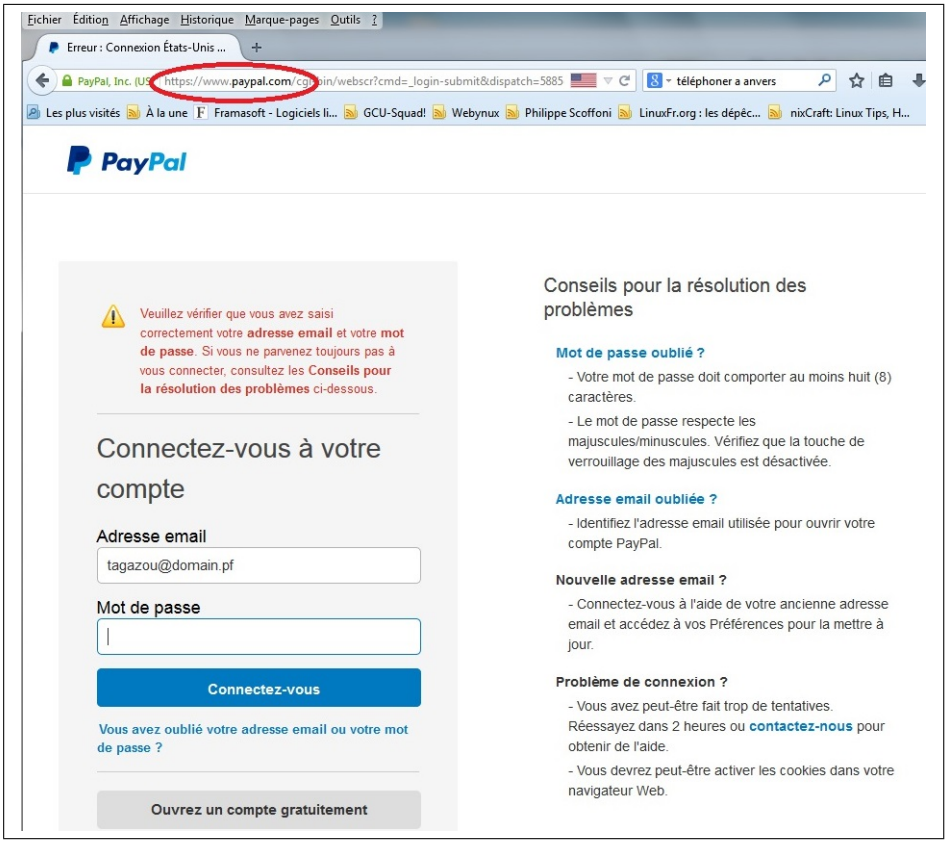
Si vous suivez mes conseils, vous ne devez même pas arriver sur cette page.

Notez bien le nom et l'adresse fournis. On trouve des chevaliers Jedi en Belgique. Rue de l'endroit à Anvers manque peut–être un peu d'originalité.

Si une autre occasion m'est donnée, je tenterai de faire mieux.

Ne perdez jamais votre temps à remplir ce genre de formulaire, je l'ai fait afin de l'utiliser pour la démonstration de l'imposture, mais vous ne devez jamais le faire.

Les techniques des pirates évoluent sans cesse et on ne sait pas de quoi ces gens sont capables.


Fichier Édition Affichage Historique Marque-pages Outils ?
Erreur : Connexion États-Unis ...
PayPal, Inc. (US
https://www.paypal.com/cgi-bin/webscr?cmd=_login-submit&dispatch=5885
téléphoner a anvers
Les plus visités
À la une
Framasoft - Logiciels li...
GCU-Squad!
Webynux
Philippe Scoffoni
LinuxFr.org : les dépêc...
nixCraft: Linux Tips, H...
PayPal
Veuillez vérifier que vous avez saisi correctement votre adresse email et votre mot de passe. Si vous ne parvenez toujours pas à vous connecter, consultez les Conseils pour la résolution des problèmes ci-dessous.
Connectez-vous à votre compte
Adresse email
tagazou@domain.pf
Mot de passe
Connectez-vous
Vous avez oublié votre adresse email ou votre mot de passe ?
Ouvrez un compte gratuitement
Conseils pour la résolution des problèmes
Mot de passe oublié ?
- Votre mot de passe doit comporter au moins huit (8) caractères.
- Le mot de passe respecte les majuscules/minuscules. Vérifiez que la touche de verrouillage des majuscules est désactivée.
Adresse email oubliée ?
- Identifiez l'adresse email utilisée pour ouvrir votre compte PayPal.
Nouvelle adresse email ?
- Connectez-vous à l'aide de votre ancienne adresse email et accédez à vos Préférences pour la mettre à jour.
Problème de connexion ?
- Vous avez peut-être fait trop de tentatives. Réessayez dans 2 heures ou contactez-nous pour obtenir de l'aide.
- Vous devrez peut-être activer les cookies dans votre navigateur Web.

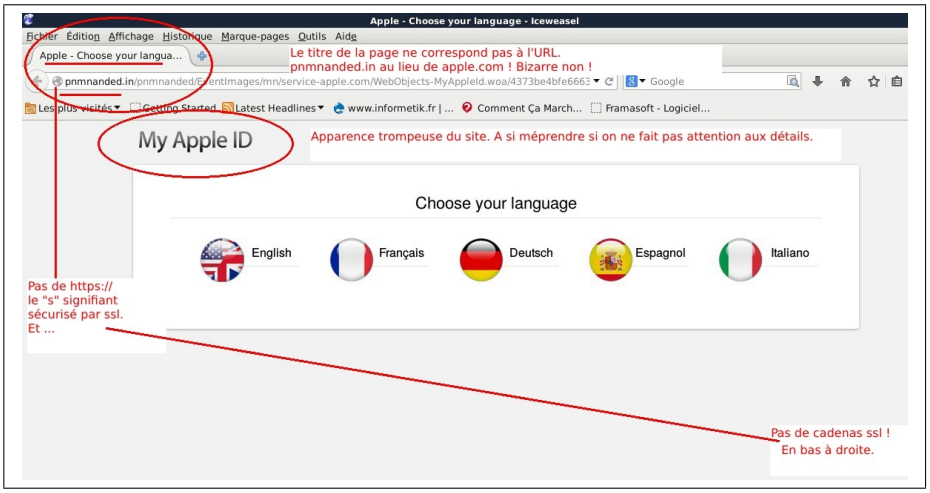
Ci-dessous, après avoir entré les informations, bien-sûr totalement fausses et inventées, je suis renvoyé automatiquement sur le vrai site de Paypal qui lui, est bien en https. Ainsi, les victimes ne se rendent même pas compte de leur méprise et ne sont pas capables de se rappeler quand elles ont été escroquées.

Si je n'étais pas attentif à la sécurité, je pense que je n'aurai pas vu la différence, pourtant elle est frappante et en premier lieu, le fait d'utiliser le protocole https.

Vol d'informations bancaires - étude de cas n° 2

Si vous aviez reçu ce message et que vous aviez cliqué sur le lien, vous seriez arrivé sur un site ressemblant à un de ceux d'Apple. Le message n'est pas très réussi, mais le site l'est extrêmement bien.

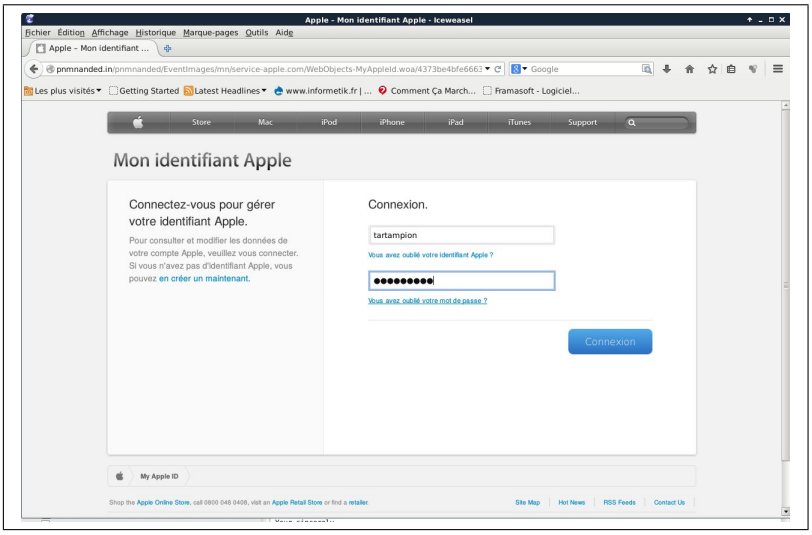
Voici le lien vers lequel mon fameux message d'Apple m'envoie



Les commentaires sont dans l'image, mais je les restitue ci-dessous :

- L'adresse située dans la barre d'adresse (URL) ne correspond pas au titre de la page. On a "pnmnanded.in/pnmnanded/" au lieu d'un site "apple.com"
- Il n'y a pas de https dans la barre d'adresse alors que le site demande une authentification.
- Il n'y a pas de cadenas en bas à droite de la fenêtre du navigateur, indiquant l'utilisation d'un protocole de communication sécurisé.

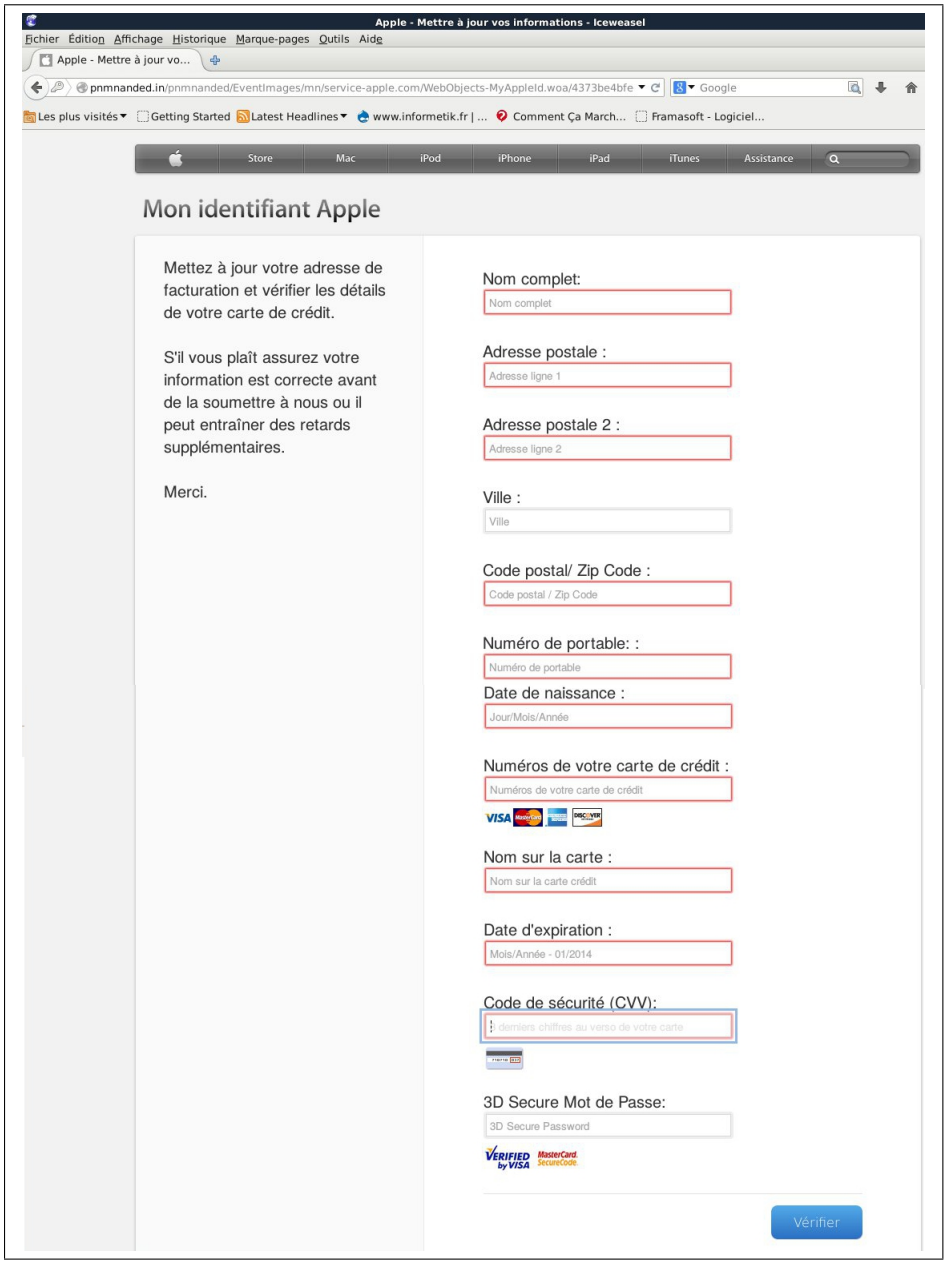
Le pire est à venir car lorsque vous êtes arrivés sur la page et que vous choisissez la langue, vous êtes envoyés vers un site dans la langue choisie qui permet de s'authentifier.



J'ai tapé un identifiant et un mot de passe bidon qui ont été acceptés, un élément qui prouve que le site est monté de toute pièce.

L'utilisateur ayant indiqué les vrais informations, se les sera fait volées à cette occasion.

Si vous saisissez n'importe quel identifiant et authentifiant bidon, il sera accepté car l'objectif est d'accéder à la page suivante pour vous voler vos informations bancaires.



Ne donnez jamais les informations demandées.

Si par mégarde, vous avez donné les informations demandées sur le faux site, vous serez ensuite redirigé vers un vrai site du vrai fournisseur (Apple, EDF, ou autre) et vous ne vous serez rendus compte de rien.

Je pense que cette démonstration suffit à donner des frissons d'horreur à toute personne un peu consciente du problème.

Ensuite, l'escroc n'aura plus qu'à utiliser votre carte bancaire dont vous lui avez généreusement donné les coordonnées, de votre plein, mais à votre

insu...

Ou, comme l'aurait dit un ancien champion de cyclisme, "à l'insu de votre plein gré".

Observez bien l'étude de cas suivante qui est encore mieux faite que celle que nous venons d'analyser.

2.2.2 Vol d'identifiant et mot de passe de messagerie

Certains sites vous voleront juste votre compte de messagerie électronique en se faisant passer pour votre fournisseur de service.

Ainsi, beaucoup de titulaires d'adresse "gmail.com" et "hotmail.com" se sont fait piéger ces dernières années, mais ce ne sont pas les seuls.

Une fois que l'escroc aura obtenu les informations demandées en se faisant passer pour le fournisseur, il changera votre mot de passe afin que vous ne puissiez plus accéder à votre messagerie, puis il enverra des messages à tout votre carnet d'adresse en racontant que vous avez eu un problème et que vous avez besoin qu'on envoie de l'argent sur tel compte, rapidement, etc.

Dans le premier cas, (vol des informations bancaires) vous vous faites plumer, dans le deuxième cas (prise de contrôle de la messagerie électronique), ce sont vos contacts dans votre carnet d'adresses qui se font plumer, mais en plus vous passez pour un ignorant et vous perdez vos amis.

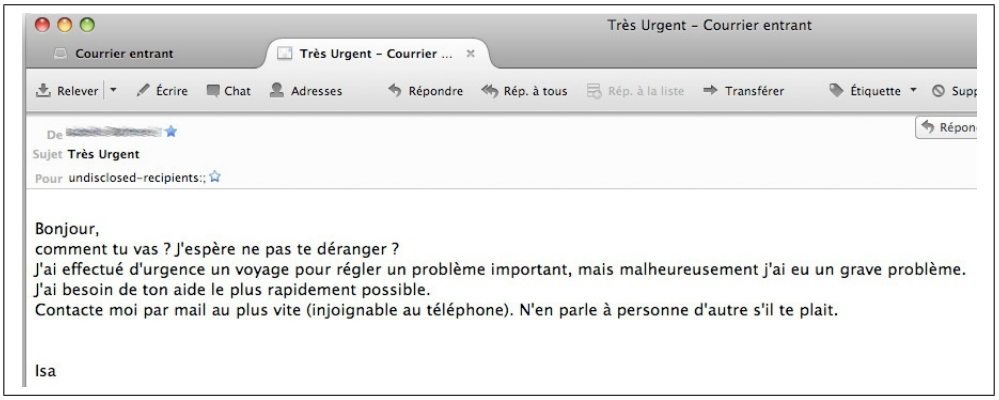
Pour se connecter à votre messagerie électronique, le pirate informatique a besoin de deux informations.

1. votre identifiant (ce qu'on appelle couramment le nom d'utilisateur)
2. votre authentifiant (ce que l'on appelle couramment le mot de passe mais qui peut être remplacé par un procédé biométrique.)

Le pirate veut vous subtiliser ces deux informations.

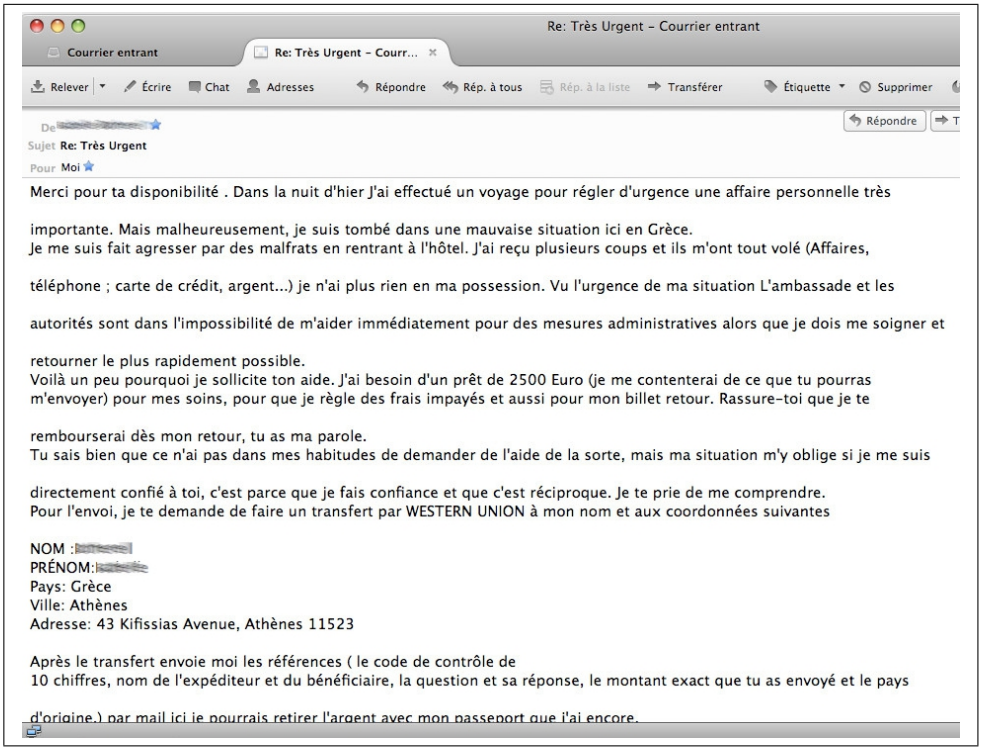
Une fois son 1^{er} objectif atteint, il a tout le loisir d'examiner le contenu de votre correspondance privée messagerie et d'envoyer des messages à tous vos contacts. Il peut même éventuellement vous faire chanter si des informations compromettantes sont trouvées.

Si vous êtes victimes d'une arnaque de ce type, voici le genre d'appel à l'aide que vos contacts recevront.


Très Urgent – Courrier entrant
Courrier entrant
Très Urgent – Courrier ...
Relever
Écrire
Chat
Adresses
Répondre
Rép. à tous
Rép. à la liste
Transférer
Étiquette
De
Sujet Très Urgent
Pour undisclosed-recipients:;
Bonjour,
comment tu vas ? J'espère ne pas te déranger ?
J'ai effectué d'urgence un voyage pour régler un problème important, mais malheureusement j'ai eu un grave problème.
J'ai besoin de ton aide le plus rapidement possible.
Contacte moi par mail au plus vite (injoignable au téléphone). N'en parle à personne d'autre s'il te plait.
Isa

Ceci est le premier message, il est alarmiste, sans donner de détails ce qui suffit à mettre le destinataire sous pression et à l'inquiéter.

Suite à la réponse au premier message, le second est plus inquiétant et assorti d'une demande de fond urgente via un système d'envoi d'argent bien connu et fréquemment utilisé par les pirates. (Western Union, ou équivalent)


Re: Très Urgent – Courrier entrant
Courrier entrant
Re: Très Urgent – Courr...
Relever
Écrire
Chat
Adresses
Répondre
Rép. à tous
Rép. à la liste
Transférer
Étiquette
Supprimer
De
Sujet Re: Très Urgent
Pour Moi
Merci pour ta disponibilité . Dans la nuit d'hier J'ai effectué un voyage pour régler d'urgence une affaire personnelle très
importante. Mais malheureusement, je suis tombé dans une mauvaise situation ici en Grèce.
Je me suis fait agresser par des malfrats en rentrant à l'hôtel. J'ai reçu plusieurs coups et ils m'ont tout volé (Affaires,
téléphone ; carte de crédit, argent...) je n'ai plus rien en ma possession. Vu l'urgence de ma situation L'ambassade et les
autorités sont dans l'impossibilité de m'aider immédiatement pour des mesures administratives alors que je dois me soigner et
retourner le plus rapidement possible.
Voilà un peu pourquoi je sollicite ton aide. J'ai besoin d'un prêt de 2500 Euro (je me contenterai de ce que tu pourras
m'envoyer) pour mes soins, pour que je règle des frais impayés et aussi pour mon billet retour. Rassure-toi que je te
rembourserai dès mon retour, tu as ma parole.
Tu sais bien que ce n'ai pas dans mes habitudes de demander de l'aide de la sorte, mais ma situation m'y oblige si je me suis
directement confié à toi, c'est parce que je fais confiance et que c'est réciproque. Je te prie de me comprendre.
Pour l'envoi, je te demande de faire un transfert par WESTERN UNION à mon nom et aux coordonnées suivantes
NOM :
PRÉNOM:
Pays: Grèce
Ville: Athènes
Adresse: 43 Kifissias Avenue, Athènes 11523
Après le transfert envoie moi les références (le code de contrôle de
10 chiffres, nom de l'expéditeur et du bénéficiaire, la question et sa réponse, le montant exact que tu as envoyé et le pays
d'origine.) par mail ici je pourrais retirer l'argent avec mon passeport que j'ai encore.

Comme indiqué plus haut, le deuxième message est plus entreprenant.

En France, l'usurpation d'identité est un délit grave, donc dans le cas où cela vous arriverait, allez impérativement porter plainte.

Si quelqu'un utilise votre identité pour nuire à autrui, la plainte vous servira de justificatif pour prouver votre bonne foi si nécessaire.

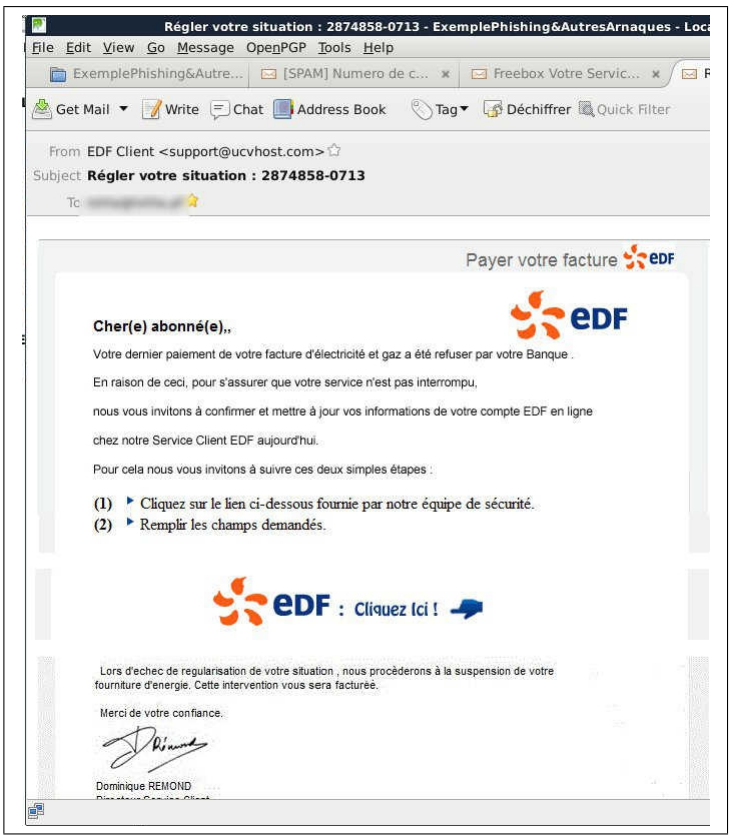
Elle pourra permettre de déclencher une enquête si les services concernés estiment qu'elle a des chances d'aboutir. (Ce qui est rare)

Elle servira également à enrichir les statistiques des attaques.

Le Phishing coûte très cher, mais mon objectif n'est pas de faire un point sur le coût du piratage, simplement de démonter les techniques utilisées afin de vous en prémunir.

2.2.3 Autre exemple

Voyez ci-dessous un autre exemple de message très réussi celui-là. Il était sensé envoyer la victime vers un site ressemblant à celui d'EDF puis incitait fortement le visiteur à saisir ses informations bancaires.


Régler votre situation : 2874858-0713 - ExemplePhishing&AutresArnaques - Loc
File Edit View Go Message OpenPGP Tools Help
ExemplePhishing&Autre...
[SPAM] Numero de c...
Freebox Votre Servic...
Get Mail
Write
Chat
Address Book
Tag
Déchiffrer
Quick Filter
From EDF Client <support@ucvhost.com>
Subject Régler votre situation : 2874858-0713
Payer votre facture EDF
EDF
Cher(e) abonné(e),,
Votre dernier paiement de votre facture d'électricité et gaz a été refuser par votre Banque .
En raison de ceci, pour s'assurer que votre service n'est pas interrompu,
nous vous invitons à confirmer et mettre à jour vos informations de votre compte EDF en ligne
chez notre Service Client EDF aujourd'hui.
Pour cela nous vous invitons à suivre ces deux simples étapes :
(1) Cliquez sur le lien ci-dessous fournie par notre équipe de sécurité.
(2) Remplir les champs demandés.
EDF : Cliquez Ici !
Lors d'echec de regularisation de votre situation , nous procèderons à la suspension de votre fourniture d'energie. Cette intervention vous sera facturée.
Merci de votre confiance.
Dominique REMOND

La première chose qui doit attirer votre attention est l'objet du message : "Réglez votre situation"

En bon français, on dirait plutôt "régularisez", mais avec le relâchement des mœurs ...

Ensuite, les autres points intéressants sont

– Ni EDF, ni Gaz de France, ni les banques, ni l'EDT, ni la reine d'Angleterre, ni le pape n'utilise le courrier électronique pour vous demander de l'argent, (Quoique le pape, je ne sais pas, je n'ai aucune relation avec lui)
– L'adresse d'expéditeur qui n'a rien à voir avec EDF,
– Si vous approchez votre souris du lien donné, vous vous apercevrez que l'URL n'a rien à voir avec EDF.

Sur ce message, si on avait cliqué sur le lien, on se serait retrouvé sur l'adresse suivante :

www.soundmagnet-band.de/includes/js/redirect.php

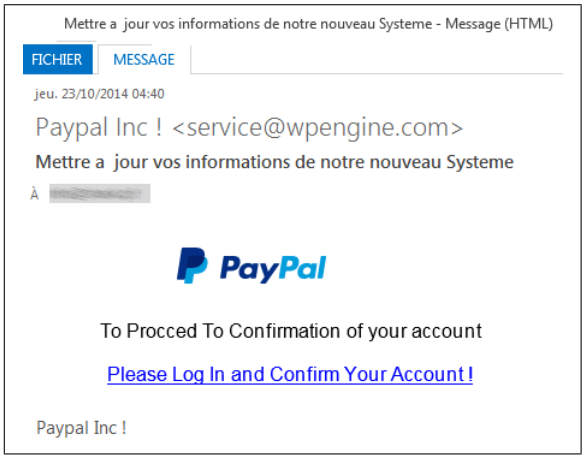
Or sur cette page, il vous serait demandé des informations relatives à votre carte bancaire, comme ce que nous avons déjà vu avec le premier cas d'hameçonnage de cette section.

2.2.4 Protections contre le phishing.

Il existe des protections contre le Phishing, parfois incluses dans des antivirus et parfois accessibles dans les réglages des navigateurs.

Ainsi, ce message reçu en octobre 2014 demande de faire une mis mise à jour des informations de compte Paypal. On peut voir dans le corps du message que l'adresse n'a rien à voir avec PayPal, malgré certaines personnes peuvent cliquer sur le lien. D'ailleurs celui-ci envoie vers un hébergement sur le serveur www.imic.ph.

Avec certains antivirus, elles auront une page à peu près comme celle figurant ci-après.

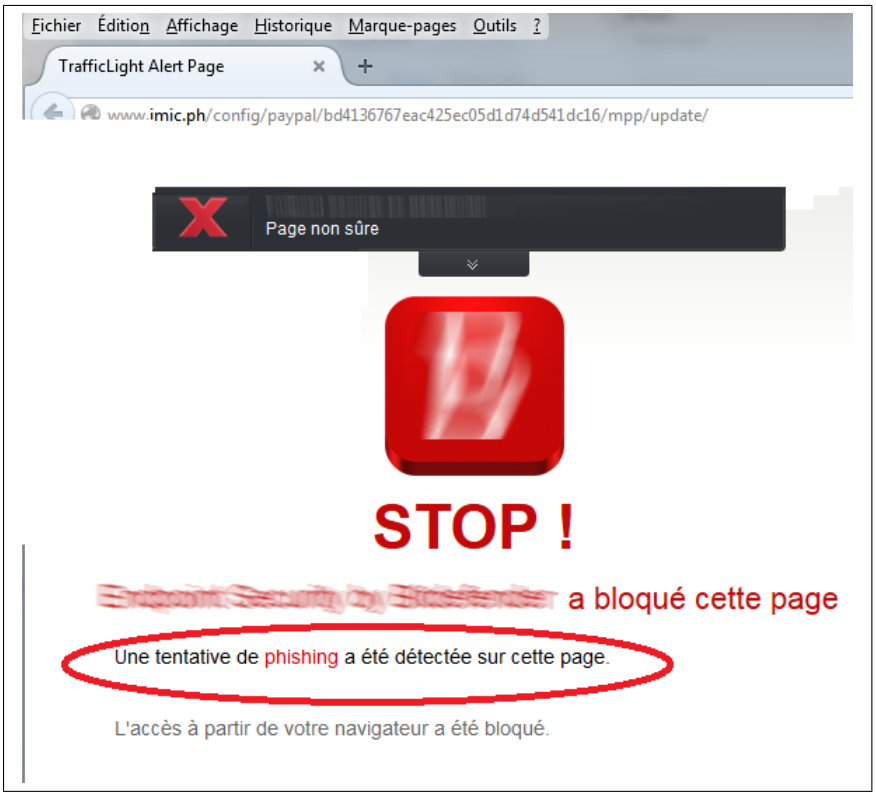

Mettre a jour vos informations de notre nouveau Systeme - Message (HTML)
FICHIER
MESSAGE
jeu. 23/10/2014 04:40
Paypal Inc ! <service@wpengine.com>
Mettre a jour vos informations de notre nouveau Systeme
À
PayPal
To Procced To Confirmation of your account
Please Log In and Confirm Your Account !
Paypal Inc !

En regardant attentivement le message, on peut remarquer des incohérences.

Dans le cas présent, si on avait cliqué sur le lien, on peut voir ce qui se serait produit sur une machine correctement protégée par un antivirus efficace et à jour.

Je ne vais pas faire de publicité pour un antivirus particulier, car celui qui est efficace aujourd'hui peut être totalement dépassé dans 6 mois, c'est pourquoi j'ai flouté la marque. En règle générale, les solutions payantes sont les plus efficaces.

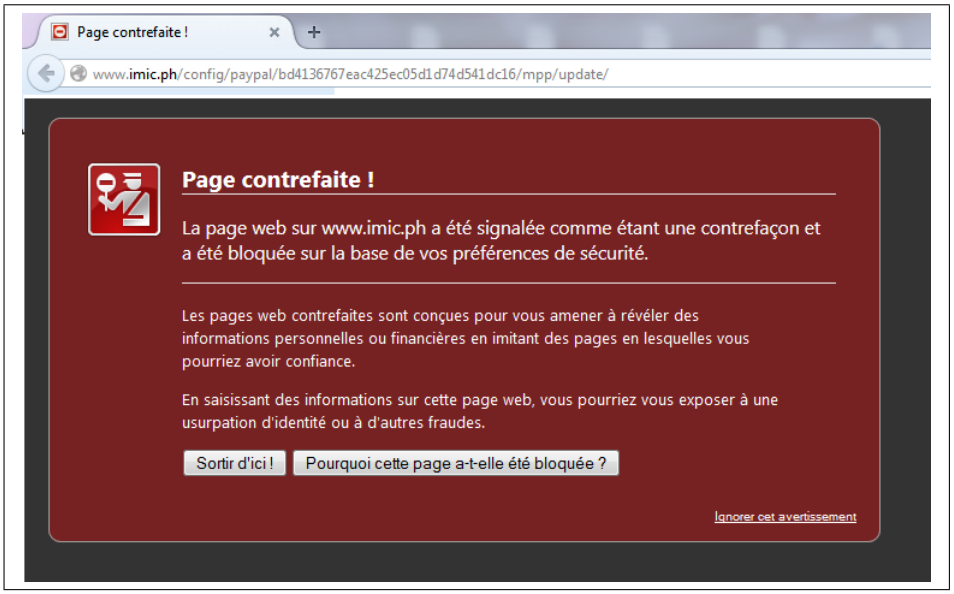
Mais la sécurité est combat permanent.


Fichier Édition Affichage Historique Marque-pages Outils ?
TrafficLight Alert Page
www.imic.ph/config/paypal/bd4136767eac425ec05d1d74d541dc16/mpp/update/
Page non sûre
STOP !
a bloqué cette page
Une tentative de phishing a été détectée sur cette page.
L'accès à partir de votre navigateur a été bloqué.

Blocage activé par un antivirus, encore faut-il qu'il soit à jour et efficace, ce qui est loin d'être toujours le cas.

On arrive bien sur le site www.imic.ph/config/paypal mais le logiciel bloque l'affichage du site et le remplace par une page spécifique.

Certains navigateurs sont tout autant capables de prendre les même initiatives, ainsi le logiciel libre Firefox, de la fondation Mozilla, (mais probablement que d'autres sont aussi efficaces en la matière) va bloquer le site et afficher également une page d'avertissement. Voir ci-dessous.


Page contrefaite !
www.imic.ph/config/paypal/bd4136767eac425ec05d1d74d541dc16/mpp/update/
Page contrefaite !
La page web sur www.imic.ph a été signalée comme étant une contrefaçon et a été bloquée sur la base de vos préférences de sécurité.
Les pages web contrefaites sont conçues pour vous amener à révéler des informations personnelles ou financières en imitant des pages en lesquelles vous pourriez avoir confiance.
En saisissant des informations sur cette page web, vous pourriez vous exposer à une usurpation d'identité ou à d'autres fraudes.
Sortir d'ici !
Pourquoi cette page a-t-elle été bloquée ?
Ignorer cet avertissement

Blocage activé par un navigateur, dans le cas présent Firefox. (On peut faire de la publicité, c'est un logiciel libre.)

Le Phishing est un fléau et de plus en plus de gens se font avoir.

Les cybercriminels se revendent ensuite les listes de cartes bleues obtenues de cette façon et il y a un véritable commerce.

Les site de revente de carte bleues sont quasiment indétectables car ils utilisent un système de navigation anonyme qui permet d'accéder à un réseau chiffré virtuel.

Ce réseau chiffré virtuel servait initialement à permettre à des personnes situées dans des pays instables ou des dictatures de s'exprimer, mais cela a très vite été exploité par les cybercriminels. Dans ce cas on parle de Darknet, expression dont vous avez peut–être déjà entendu parler.

C'est le côté obscur du réseau et je dirais même le côté obscur de T.O.R. qui est le logiciel permettant cet accès au réseau virtuel chiffré.

Ce dont il faut se souvenir :

- Ne donnez jamais les coordonnées complets de votre carte bancaire en dehors d'une transaction.
- Ne le faites jamais sur un site qui n'est pas sécurisé.
- Ne Réglez vos achats par Internet QUE sur des sites dignes de confiance.

2.3 Quelques exemples de Spam ingénieux et dangereux

2.3.1 L'ingéniosité du vaudou béninois

Le vaudou est une très ancienne religion répandue dans plusieurs pays d'Afrique de l'ouest. Le commerce triangulaire (commerce des esclaves entre le XVI^{e} et le début du XIX^{e} siècles) a répandu cette pratique religieuse jusque dans les Caraïbes et en particulier à Haïti.

Voici un message provenant de quelqu'un se prétendant guérisseur et marabout avec de très grand pouvoirs.

GRAND MARABOUT DU BENIN LA TERRE...

mer. 30/07/2014 10:46

GRAND MARABOU <avohissan.djifa1@gmail.com>

GRAND MARABOUT DU BENIN LA TERRE DE VODOUN

À

GRAND MARABOUT DU BENIN LA TERRE DE VODOUN

Je m'appelle Avohissan tradipraticien je peut intervenir dans les domaines suivants : - amour : retour de l'être aimé, maraboutage d'une femme ou d'un homme, mettre fin à un divorce, attirer quelqu'un... - chance : grigri pour avoir plus de chance aux jeux, pour être un peu moins poissard dans la vie... - travail : incantations magiques pour trouver un travail, ne pas se faire virer, rituels pour être augmenté, rituels pour réussir les entretiens d'embauche - business et affaires: grigri à utiliser quand on monte une entreprise, talisman pour mieux négocier les contrats, prières pour faire venir les clients et attirer des partenaires..
N'hésitez pas à me contacté Adresse Email: avohissan.djifa@gmail.com

Faite un clik sur le lien dessous pour regarder la video !

https://www.youtube.com/watch?v=RAxXVMhswOU

Personnellement, je ne crois pas du tout à ce genre de choses, mais l'expéditeur trouve un moyen astucieux pour donner de la crédibilité à son message et j'imagine que quelqu'un qui aurait un moment de faiblesse pourrait se laisser impressionner.

Pour donner du crédit à une affirmation fausse, il suffit de détourner une image ou une séquence vidéo comme on peut le voir ci-dessous avec cet extrait de document réalisé par la chaîne culturelle franco–allemande Arte.

Télécharger une vidéo depuis le site de vidéo en ligne Youtube est relativement simple avec quelques logiciels libres ou un plug-in sous le navigateur "Firefox". Il faut avoir un compte sur Youtube, que n'importe qui peut créer gratuitement.

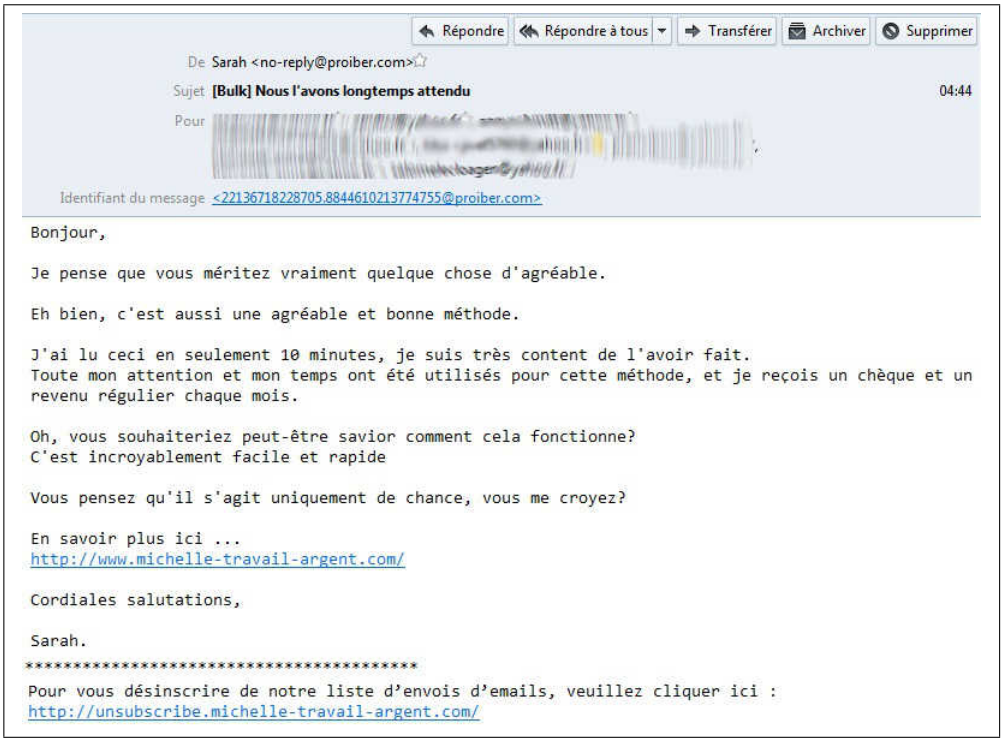
Cette pratique est relativement simple à mettre en œuvre, l'escroc a simplement téléchargé la vidéo et l'a rechargé sous son propre compte

en faisant croire que les services qu'il prétend proposer ont un lien avec le film.

Le lien fournit à la fin du message envoie vers cette séquence vidéo d'un documentaire d'Arte, dans l'objectif de détourner le sens de celui-ci pour donner du crédit à son message.

2.3.2 Faire de l'argent facilement en se faisant plumer ...

Certains messages promettent de l'argent facile, comme celui présenté ci-dessous.


Répondre | Répondre à tous | Transférer | Archiver | Supprimer

De Sarah <no-reply@proiber.com>

Sujet **[Bulk] Nous l'avons longtemps attendu** 04:44

Pour [redacted]

Identifiant du message <221367182287O5.8844610213774755@proiber.com>

Bonjour,

Je pense que vous méritez vraiment quelque chose d'agréable.

Eh bien, c'est aussi une agréable et bonne méthode.

J'ai lu ceci en seulement 10 minutes, je suis très content de l'avoir fait.
Toute mon attention et mon temps ont été utilisés pour cette méthode, et je reçois un chèque et un revenu régulier chaque mois.

Oh, vous souhaiteriez peut-être savior comment cela fonctionne?
C'est incroyablement facile et rapide

Vous pensez qu'il s'agit uniquement de chance, vous me croyez?

En savoir plus ici ...
http://www.michelle-travail-argent.com/

Cordiales salutations,

Sarah.

****

Pour vous désinscrire de notre liste d'envois d'emails, veuillez cliquer ici :
http://unsubscribe.michelle-travail-argent.com/

Mettons les choses au clair, l'argent facile est forcément de l'argent malhonnête et de toute façon, avec ce genre de site, vous ne réussirez qu'à vous faire plumer intégralement jusqu'au duvet.

Perdre de l'argent en voulant en gagner, c'est un peu dommage...

Une fois sur le site, on vous donnera quelques explications qui vous donneront envie de continuer, puis une fois que le visiteur crédule est convaincu, on lui demande d'envoyer de l'argent pour accéder à la méthode.

Nouvel onglet
Maman Gagne Des Sous
www.michelle-travail-argent.com
LA MÉTHODE QUI A CHANGÉ MA VIE.
Se faire un revenu régulier de la maison
est plus facile que jamais.
C'est simple ! C'est légal ! C'est rapide !
michellebonne73@mail.com
Bonjour,
Mon nom est Michele. J'ai trois beaux
garçons et malheureusement j'ai perdu mon mari
dans un accident de voiture il y a cinq ans.
Avant cette tragédie, je travaillais
comme développeur Web dans une société de
jeux en ligne. La vie était belle, nous avions
des bons revenus qui rentraient Les enfants
étaient heureux d'avoir leur papa à leurs
côtés, qui les aidaient, qui jouaient avec eux,
et qui leur préparait leurs plats préférés.
J'étais heureuse de m'en sortir dans
toutes les tâches de "maman" et le plus
important, nous avions le week-end pour
voyager et passer du temps ensemble
comme toute famille.
Mais alors, c'est arrivé, sans crier gare,
L'amour de ma vie n'est plus !
Les gains réalisés
par mes abonnés au
cours des 2 derniers mois
500,330€
Nouveau chapitre ! Une nouvelle vie ! De nouveaux arrangements !
Comme vous le comprenez sans doute, je devais trouver un moyen de procurer à mes enfants tout ce
dont ils avaient besoin et bien sûr d'être avec eux autant que je le pouvais.
J'ai alors eu une idée brillante.
Je connaissais bien le jeu en ligne de par mon experience de web-développeur, et j'avais déjà analysé
un moyen de battre la roulette, donc je me suis dit "Hé pourquoi ne pas faire un essai ?"
J'ai décidé de tenter le coup ! Ce qui a commencé par hasard, a terminé comme l'une des choses les
plus importantes que j'ai jamais accomplies. Aujourd'hui, je ne passe pas plus de 30 minutes dans
chaque casino, et mes gains énormes m'ont permis d'arrêter mon travail et de travailler à domicile.
Pourquoi je partage avec vous ma méthode pour gagner de l'argent ?
Simplement, parce qu'il y a tellement de gens que la vie a traités injustement et je sentais que ce
moyen simple de faire de l'argent devait être partagé partout dans le monde. Comprenez, aider les
autres ne me fait gagner ni plus ni moins, je me sens juste bien de savoir que d'autres peuvent avoir
une bonne vie, partir avec leurs familles en vacances, passer plus de temps à la maison avec leurs
enfants, et s'acheter tout ce qu'ils veulent.

Dans le cas présent, le lien envoie vers un site de Casino en ligne sur lequel il faut verser 65 euros pour commencer et il y a également d'autres pages explicatives sur la méthode bidon sensée battre la roulette et présentée comme 100% légale.

Grâce à un petit outil installé sur mon navigateur, je peux savoir où est hébergé le site, or il apparait comme étant en Russie. (Le petit drapeau à droite de l'URL en témoigne) Cependant, il est possible qu'il soit à un endroit totalement différent car les cybercriminels utilisent souvent le Darknet [3] pour brouiller les pistes.

3. Le darknet est une sorte de réseau virtuel chiffré utilisé au départ pour favoriser la libre expression dans les dictatures ou les pays instables et dont l'usage a été détourné par les réseaux criminels. Ce réseau virtuel chiffré utilise les même infrastructures matérielles que le réseau Internet ordinaire.

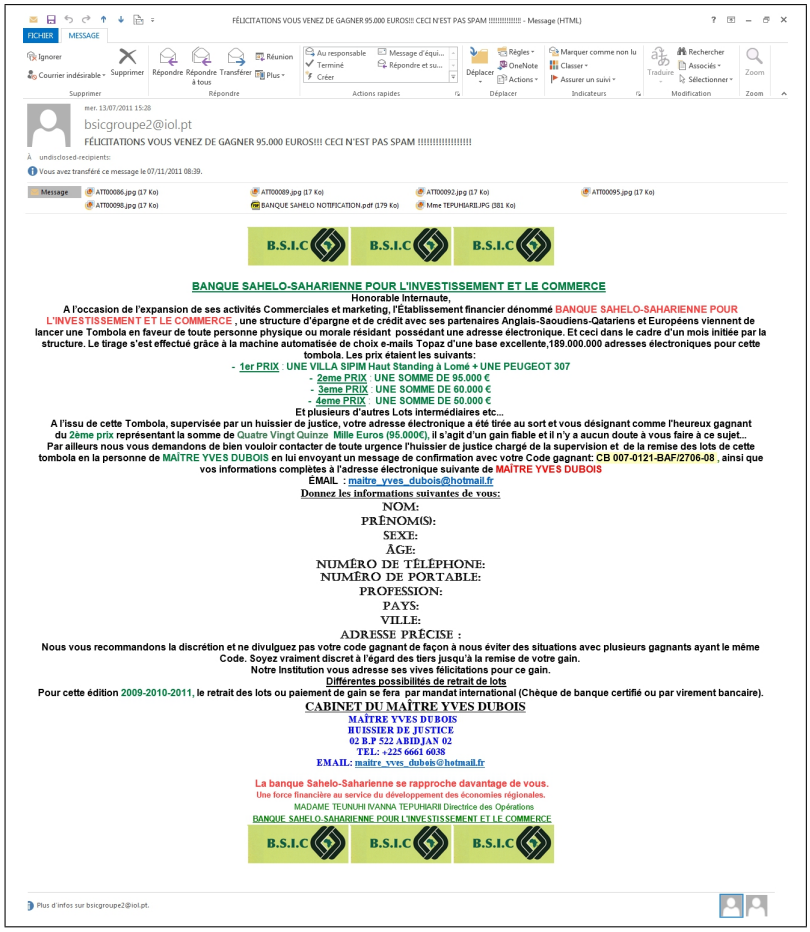
Si le site est réellement en Russie, c'est un magnifique pays dans lequel malheureusement, règnent en maîtres Vladimir Poutine et les réseaux mafieux.

J'ignore lequel des deux est le pire, mais n'imaginez pas gagner de l'argent avec ces gens là, ce ne sont pas des philanthropes.

Passez donc votre chemin et ne donnez surtout pas votre démission, vous pouvez encore avoir besoin de votre travail !

2.4 Analyse d'un document – SCAM

Le message ci-dessous est un scam.



FÉLICITATIONS VOUS VENEZ DE GAGNER 95.000 EUROS!!! CECI N'EST PAS SPAM !!!!!!!!!!!!!!!!! - Message (HTML)

bsicgroupe2@iol.pt

FÉLICITATIONS VOUS VENEZ DE GAGNER 95.000 EUROS!!! CECI N'EST PAS SPAM !!!!!!!!!!!!!!!!!

B.S.I.C B.S.I.C B.S.I.C

BANQUE SAHELO-SAHARIENNE POUR L'INVESTISSEMENT ET LE COMMERCE

Honorable Internaute,

A l'occasion de l'expansion de ses activités Commerciales et marketing, l'Établissement financier dénommé BANQUE SAHELO-SAHARIENNE POUR L'INVESTISSEMENT ET LE COMMERCE , une structure d'épargne et de crédit avec ses partenaires Anglais-Saoudiens-Qatariens et Européens viennent de lancer une Tombola en faveur de toute personne physique ou morale résidant possédant une adresse électronique. Et ceci dans le cadre d'un mois initiée par la structure. Le tirage s'est effectué grâce à la machine automatisée de choix e-mails Topaz d'une base excellente,189.000.000 adresses électroniques pour cette tombola. Les prix étaient les suivants:

- 1er PRIX : UNE VILLA SIPIM Haut Standing à Lomé + UNE PEUGEOT 307
- 2eme PRIX : UNE SOMME DE 95.000 €
- 3eme PRIX : UNE SOMME DE 60.000 €
- 4eme PRIX : UNE SOMME DE 50.000 €

Et plusieurs d'autres Lots intermédiaires etc...

A l'issu de cette Tombola, supervisée par un huissier de justice, votre adresse électronique a été tirée au sort et vous désignant comme l'heureux gagnant du 2ème prix représentant la somme de Quatre Vingt Quinze Mille Euros (95.000€), il s'agit d'un gain fiable et il n'y a aucun doute à vous faire à ce sujet... Par ailleurs nous vous demandons de bien vouloir contacter de toute urgence l'huissier de justice chargé de la supervision et de la remise des lots de cette tombola en la personne de MAÎTRE YVES DUBOIS en lui envoyant un message de confirmation avec votre Code gagnant: CB 007-0121-BAF/2706-08 , ainsi que vos informations complètes à l'adresse électronique suivante de MAÎTRE YVES DUBOIS

EMAIL : maitre_yves_dubois@hotmail.fr

Donnez les informations suivantes de vous:

NOM:
PRÉNOM(S):
SEXE:
ÂGE:
NUMÉRO DE TÉLÉPHONE:
NUMÉRO DE PORTABLE:
PROFESSION:
PAYS:
VILLE:
ADRESSE PRÉCISE :

Nous vous recommandons la discrétion et ne divulguez pas votre code gagnant de façon à nous éviter des situations avec plusieurs gagnants ayant le même Code. Soyez vraiment discret à l'égard des tiers jusqu'à la remise de votre gain.

Notre Institution vous adresse ses vives félicitations pour ce gain.

Différentes possibilités de retrait de lots

Pour cette édition 2009-2010-2011, le retrait des lots ou paiement de gain se fera par mandat international (Chèque de banque certifié ou par virement bancaire).

CABINET DU MAÎTRE YVES DUBOIS

MAÎTRE YVES DUBOIS
HUISSIER DE JUSTICE
02 B.P 522 ABIDJAN 02
TEL: +225 6661 6038
EMAIL: maitre_yves_dubois@hotmail.fr

La banque Sahelo-Saharienne se rapproche davantage de vous.
Une force financière au service du développement des économies régionales.
MADAME TEUNUHI IVANNA TEPUHARII Directrice des Opérations
BANQUE SAHELO-SAHARIENNE POUR L'INVESTISSEMENT ET LE COMMERCE

B.S.I.C B.S.I.C B.S.I.C

Pour analyser et comprendre un document, il faut d'abord l'avoir vu.

Qu'est-ce qu'un "scam" ?

Il existe plusieurs catégories de messages frauduleux, parmi lesquels le scam ou arnaque à la nigériane car sous la pression de plusieurs pays

anglophone, c'est le Nigéria qui a le premier légiféré contre ce type de délinquance.

Définition d'un scam : "cyber-arnaques" ou "cyber-escroqueries" généralement envoyée par courriel. On les appelle arnaques à la nigériane car c'est ce pays qui a légiféré le premier sous la pression d'autres états anglophone. On dit parfois arnaque 419 ou scam 419 en référence au numéro de l'article de loi. Ces courriels vous sollicitent pour récupérer des sommes importantes en échange d'un pourcentage. Ils proviennent de pays en voie de développement et sont souvent rédigés depuis des cybercafés.

Ils coûtent parfois très cher aux victimes et cela peut aller jusqu'à la mort car certaines victimes ont été poussées au suicide.

D'autres victimes voulant récupérer leur argent sont allé jusqu'à avoir un rendez–vous avec les arnaqueurs et ils ont été pris en otage. Ce qui n'est pas très malin vous en conviendrez.

Regardez le document joint fourni en première page :

La première chose qui doit attirer votre attention est l'objet du message :
"FELICITATION VOUS VENEZ DE GAGNER"

La deuxième chose qui doit attirer votre attention, dans l'entête est "CECI N'EST PAS UN SPAM ! ! !"

Et bien voyons... devant une telle affirmation, j'aurais tendance à demander si ce n'est pas de la carotte rapée ou du chou farci !

C'est un scam et la définition du scam entre dans celle du spam, donc c'est un spam.

Si je me présente à vous et que je vous dis que je ne suis pas tueur à gage, méfiez–vous !

Autre point pouvant attirer l'attention :

Le nom de la banque. Il pourrait arriver que vous receviez ce type de message d'une banque moins exotique. Méfiez–vous tout autant car aucune banque ne vous enverra jamais ce type de message, malheureusement.

Les prix offerts aux gagnants sont relativement gros, ce qui doit étonner le lecteur du message.

Le tout est rendu crédible par le nom d'un huissier de justice accompagné de son adresse de courriel. Et c'est bien un des éléments qui accrochera les plus crédules.

Ils vont écrire à l'huissier de justice qui leur dira qu'en effet tout est vrai.

Mais, cette adresse d'huissier de justice est fausse. Cela ne veut pas dire que l'huissier n'existe pas, mais s'il existe, il ignore tout du trafic qui se déroule en son nom.

N'oubliez jamais qu'on ne peut pas savoir qui se trouve derrière une adresse électronique.

Il existe peut–être un véritable Maître Yves DUBOIS à Abidjan, mais j'en doute fort. Et si c'est le cas, le vérifier est un peu compliqué pour le commun des mortels.

Autre élément d'usurpation d'identité que vous devez connaître. Joint à ce message se trouvait la copie de la carte d'identité d'une personne avec un nom tahitien dont je ne donne que le début "TEPU".

J'ai volontairement flouté la carte, mais la copie était très nette dans le message.

Cette personne a peut–être été une victime de ces escrocs et au cours des échanges, afin d'obtenir de plus en plus d'information et de bien

profiter de leur victime, ils ont demandé à cette dame une copie de sa carte d'identité, puis une fois leur méfait accompli, ils l'ont utilisée.

Notez bien que Madame "TEPUxxxxxx" est domiciliée à Afaahiti sur l'île de Tahiti. On notera bien que le message étant destiné aux internautes de Polynésie française, le fait de donner un peu plus de crédibilité au message en prenant le nom d'une personne du même territoire fait probablement aussi partie de la technique de manipulation.

Il y a d'autres éléments dans ce message qui peuvent vous inciter à vous poser des questions.

On vous demande votre état civil.

Pourquoi faire, puisque j'ai gagné ?

Si j'ai gagné c'est qu'on me connaît !

Alors pourquoi ont-ils besoin de tout cela ?

Ils finiront par vous dire que pour encaisser l'argent ils ont besoin qu'on leur envoie une certaine somme, puis une autre et encore une autre, jusqu'à ce que la victime comprenne.

Confus de honte de s'être fait berner de la sorte, la plupart des gens ne portent pas plainte.

C'est un tort. Il est normal d'avoir honte devant la grosseur des ficelles, mais il faut stopper ce genre de trafic.

Le message analysé ici est très compliqué et très riche, mais il en existe des beaucoup plus simple dont il faut tout autant se méfier.

mar. 12/08/2014 04:08
directionservice.2014@ig.com.br
A votre Attention Mr / Mme vous êtes bénéficiaire LEO-CLUB INTERNATIONAL

À undisclosed-recipients:

LOTERIE LEO-CLUB INTERNATIONAL

Bonjour cher(e) lauréat(e)

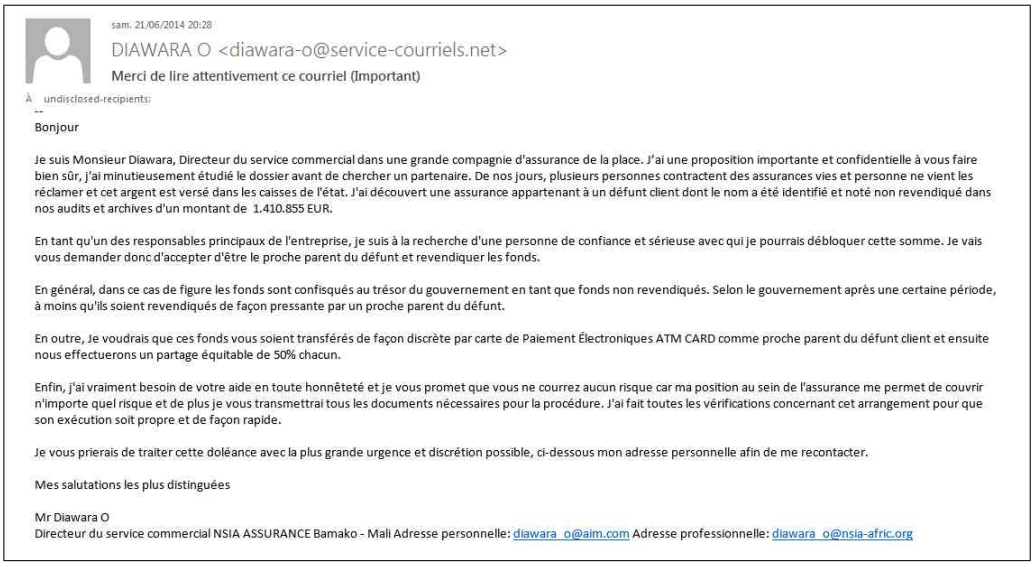
Nous venons par ce présent courriel vous informer de votre gain de 170.000€
par la loterie LEO-CLUB INTERNATIONAL en partenariat avec LION'S GATE dans le cadre de la promotion de ses activités humanitaires.

Ceci n'étant donc pas un spam ni un virus nous vous prions de vous rendre dès réception de cette notification sur le site officiel : http://www.leo-club.org/ pour plus d'informations puis remplir le formulaire qui vous permettra d'entamer toute procédure de retrait de votre gain à l'aide de votre code gagnant : 789-866.

Veuillez recevoir cher(e) lauréat(e) toutes nos félicitations et l'expression de nos salutations les plus sincères.

Voici encore un exemple de faux message de loterie à laquelle vous n'avez jamais joué.

Voici quelques autres exemples parmi lesquels vous retrouverez des éléments de manipulation tels que ceux évoqués précédemment.



sam. 21/06/2014 20:28
DIAWARA O <diawara-o@service-courriels.net>
Merci de lire attentivement ce courriel (Important)

À undisclosed-recipients:

--

Bonjour

Je suis Monsieur Diawara, Directeur du service commercial dans une grande compagnie d'assurance de la place. J'ai une proposition importante et confidentielle à vous faire bien sûr, j'ai minutieusement étudié le dossier avant de chercher un partenaire. De nos jours, plusieurs personnes contractent des assurances vies et personne ne vient les réclamer et cet argent est versé dans les caisses de l'état. J'ai découvert une assurance appartenant à un défunt client dont le nom a été identifié et noté non revendiqué dans nos audits et archives d'un montant de 1.410.855 EUR.

En tant qu'un des responsables principaux de l'entreprise, je suis à la recherche d'une personne de confiance et sérieuse avec qui je pourrais débloquer cette somme. Je vais vous demander donc d'accepter d'être le proche parent du défunt et revendiquer les fonds.

En général, dans ce cas de figure les fonds sont confisqués au trésor du gouvernement en tant que fonds non revendiqués. Selon le gouvernement après une certaine période, à moins qu'ils soient revendiqués de façon pressante par un proche parent du défunt.

En outre, Je voudrais que ces fonds vous soient transférés de façon discrète par carte de Paiement Électroniques ATM CARD comme proche parent du défunt client et ensuite nous effectuerons un partage équitable de 50% chacun.

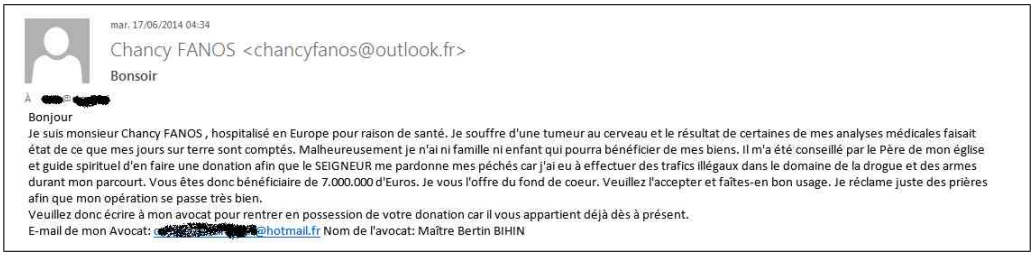
Enfin, j'ai vraiment besoin de votre aide en toute honnêteté et je vous promet que vous ne courrez aucun risque car ma position au sein de l'assurance me permet de couvrir n'importe quel risque et de plus je vous transmettrai tous les documents nécessaires pour la procédure. J'ai fait toutes les vérifications concernant cet arrangement pour que son exécution soit propre et de façon rapide.

Je vous prierais de traiter cette doléance avec la plus grande urgence et discrétion possible, ci-dessous mon adresse personnelle afin de me recontacter.

Mes salutations les plus distinguées

Mr Diawara O
Directeur du service commercial NSIA ASSURANCE Bamako - Mali Adresse personnelle: diawara_o@aim.com Adresse professionnelle: diawara_o@nsia-afric.org

Un message d'un escroc qui insiste lourdement au point d'envoyer un courriel par jour. Insister fait probablement parti de la technique.



mar. 17/06/2014 04:34

Chancy FANOS <chancyfanos@outlook.fr>

Bonsoir

À [redacted]

Bonjour

Je suis monsieur Chancy FANOS , hospitalisé en Europe pour raison de santé. Je souffre d'une tumeur au cerveau et le résultat de certaines de mes analyses médicales faisait état de ce que mes jours sur terre sont comptés. Malheureusement je n'ai ni famille ni enfant qui pourra bénéficier de mes biens. Il m'a été conseillé par le Père de mon église et guide spirituel d'en faire une donation afin que le SEIGNEUR me pardonne mes péchés car j'ai eu à effectuer des trafics illégaux dans le domaine de la drogue et des armes durant mon parcourt. Vous êtes donc bénéficiaire de 7.000.000 d'Euros. Je vous l'offre du fond de coeur. Veuillez l'accepter et faîtes-en bon usage. Je réclame juste des prières afin que mon opération se passe très bien.

Veuillez donc écrire à mon avocat pour rentrer en possession de votre donation car il vous appartient déjà dès à présent.

E-mail de mon Avocat: [redacted]@hotmail.fr Nom de l'avocat: Maître Bertin BIHIN

Encore un qui est à l'hôpital, près de mourir et qui pense à moi.

Réflechissons en cœur un bref instant :

- Si j'étais dans un hôpital, avec un cancer en phase terminale, penserais-je vraiment à moi ?
- Oui, je penserai à moi, mais certainement à un inconnu du bout du monde qui ne me connait pas.

2.4.1 Cas particulier des offres de prêt

Les offres de prêts entre particuliers s'apparentent au SCAM.

Offre de prêt sérieux et rapide - Message...

dim. 03/08/2014 05:24

patricia delpirla <patricia.deprestamos@gmail.com>

Offre de prêt sérieux et rapide

À undisclosed-recipients:

Offre de prêt sérieux et rapide

Vous aviez besoin de prêts d'argent entre particuliers pour faire face aux difficultés financières pour enfin sortir de l'impasse que provoquent les banques, par le rejet de vos dossiers de demande de crédits,prêt. Je suis Mm Eva BORDONES particulier d'experts financiers en mesure de vous faire un prêt au montant dont vous avez besoin et avec des conditions très simple qui vous faciliteront la vie. Si vous avez vraiment besoin de prêt, Veuillez me contacter directement par Email: bordones_financieroservicio@live.fr <mailto:bordones_financieroservicio@live.fr>

Pour débloquer l'argent proposé il faut envoyer des informations qui une fois communiquées vont faire que l'internaute se sentira piégé.

De eva doriangeli Bordones rodriguez
Répondre | Transférer | Archiver | Indésirable | Supprimer
Sujet **RE: crédit d'abonnement au prêt d'argent.** 05/08/2014 09:54
Pour Moi
Identifiant du message <DUB123-W160BA94B2CB5E7C14A218A87E30@phx.gbl>
En réponse à
Références
X-Account-Key account3

Bonjour M.
je viens de lire votre message et je tiens à vous parler de marchandises que je veux première remplir ce formulaire afin que je puisse vous donner votre paramètre de forme de crédit d'abonnement à prêter d'argent.

PRÉNOM:.....
NOM:.....
ÂGE:.....
ÉTAT MATRIMONIAL:.....

ADRESSE COMPLÈTE :.....
VILLE:.....
PAYS:.....
PROFESSION:.....

SALAIRE MENSUEL :.....
INDICATIF DE VOTRE PAYS.....
NUMÉRO DE TÉLÉPHONE MOBILE : .....

NUMÉRO DE TÉLÉPHONE:.....
MONTANT DU PRÊT :.....

BUT du prêt : .....
durée de l'amortissement (très important):.....
MODE DE TRANSFERT DEMANDÉ:.....

NUMÉRO DE CARTE D'IDENTITÉ:.....

Seul sachant que cette information sera vérifiée, est exige que vous remplissiez tout point par point ces informations pour l'enregistrement de votre demande dans notre base de données.

MERCI DE VOTRE COMPRÉHENSION

Ensuite il faudra payer des frais de dossier qui vont dans la poche de l'escroc, mais jamais l'argent ne sera débloqué.

Je dois attirer votre attention sur l'utilisation de plus en plus régulière des réseaux sociaux pour faire passer ce genre de messages.

Voyez l'exemple ci-dessous sur un fameux site de réseaux sociaux dont le nom commence par un F.

Offres de prêt entre particulier
il y a 8 heures

Bonjour
Je suis un particulier un agent retraitée de l'UNICEF et compte tenu de la crise économique actuelle j'aimerais sincèrement et franchement aider toute la population du monde entier qui sont dans le besoin d'argent donc je décide de faire des prets a toute personne interressé.
Vous avez des difficultés financières. Les portes se ferment devant vous.
Vous ne savez plus comment faire pour améliorer votre situation.
Je vous propose sans aucun engagement de votre part, d'étudier votre situation.
Vous recherchez un prêt dans ces diverses domaines :
- Crédit Immobilier
- Crédit pour les travaux
- Crédit de consommation
- Rachat de crédits
- Crédit relais
- Crédit Permanent

Pourquoi ne pas le faire avec un professionnel qui a des conditions préférentielles.
Etudions ensemble votre situation et voyons ce que nous pouvons faire
Pour toute information veuillez me contacter par mail : Email: marois.meleine@hotmail.fr

Email: marois.meleine@hotmail.fr
- Nos atouts -
- Réponse rapide en moins de 24/H
- Sans engagement
- Demande gratuite

Une dernière offre de prêt reçue par courriel récemment et qui est traduite dans plusieurs langues.

lun. 11/08/2014 10:56

P2P FINANCE-PLUS <jmapierrot@gmail.com>

À [redacted]

FRANCAIS

Salut !
Vous,particuliers en France,Canada,Belgique,Portugal,Italie ou n'importe où dans le monde entier... si vous avez besoin d'avoir une aide financière (prêt d'argent) dans l'un des domaines suivant:
- Financement
- Prêts immobiliers
- Prêts à l'investissement
- Prêt automobile
- Dette de consolidation
-Marge de crédit
-Prêts personnels
-Autre type de prêt
Ne vous inquiétez plus!!
Nous offrons à toute personne majeur,responsable et de bonne moralité,des prêts d'argent ou financement à court,moyen ou long terme. N'hésitez donc pas à nous contacter pour toutes vos demandes de prêts.
Nous octroyons des prêt allant de 5000 à 800 000€. sécurité et confidentialité garanties. Nos Transactions sont appuyées et certifiées par acte du notaire. Laissez-nous vous aider alors contacter nous maintenant et soumettez nous vos demandes.
Conditions:
- Avoir au moins 20 ans
- Avoir un revenu mensuel régulier
- Être une personne de bonne moralité
- Être capable de rembourser l'argent emprunté

P2P FINANCE-PLUS **Alors,pourquoi attendre???!!**

Contactez-nous dès maintenant:
e-mail: p2pfinanceplus@financier.com
Tél: +33 (0) 6 84 37 43 53

ENGLISH

P2P FINANCE-PLUS

2.4.2 Cas particuliers des "lovescam"

Les "Love Scam", comme leur nom l'indiquent, profitent du sentiment de solitude de certaines personnes pour leur faire miroiter des rencontres moyennant finance. Ce petit jeu peut avoir des conséquences dramatiques lorsque la victime a commencé à communiquer des informations sensibles ou des photographies par webcam, par exemple.

Le fonctionnement est le même que dans le cas des Scam classiques.

2.5 Analyse d'un document comportant une pièce jointe infectée

Cette section va nous permettre de comprendre comment vous prémunir d'une pièce jointe infectée dans un message et pourquoi vous ne risquez rien tant que vous n'ouvrez pas ladite pièce jointe.

Gloablement le spam est un courrier indésirable ou pourriel (office québecois de la langue française)

Comme nous l'avons vu, certains pourriels peuvent contenir des pièces jointes. Il arrive que ces fichiers contiennent des petits programmes malveillants dont certains peuvent avoir un effet catastrophique sur votre système.

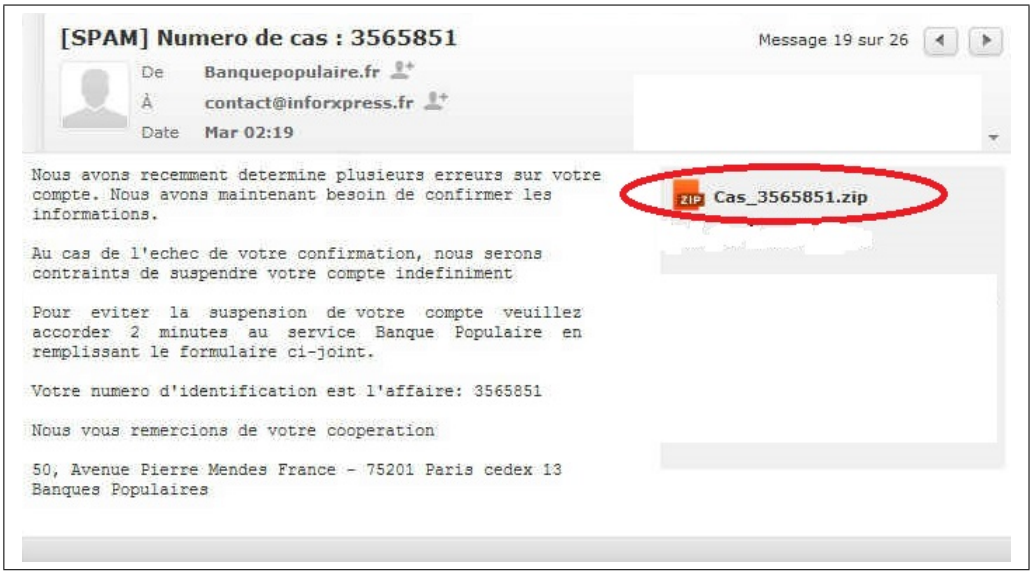
2.5.1 Un bel exemple de pièce jointe infectée ci-dessous.

Les virus de messagerie commencent à se répandre depuis les années 90, certains d'entre eux sont devenus assez complexes et peuvent avoir des effets dévastateurs, obligeant les victimes à réinstaller totalement leur machine.

En ce moment circulent sur Internet un certain nombre de messages contenant des "rançongiciels."

A l'aide d'un système particulier, j'ai analysé la pièce jointe et j'ai pu découvrir qu'elle contenait effectivement un logiciel malveillant.

Ne cherchez jamais à analyser les pièces jointes, même pour tester votre antivirus. Il existe des procédures spéciales pour cela avec des fichiers leurres spéciaux.


[SPAM] Numero de cas : 3565851
Message 19 sur 26
De Banquepopulaire.fr
À contact@inforxpress.fr
Date Mar 02:19
Nous avons recemment determine plusieurs erreurs sur votre compte. Nous avons maintenant besoin de confirmer les informations.
Au cas de l'echec de votre confirmation, nous serons contraints de suspendre votre compte indefiniment
Pour eviter la suspension de votre compte veuillez accorder 2 minutes au service Banque Populaire en remplissant le formulaire ci-joint.
Votre numero d'identification est l'affaire: 3565851
Nous vous remercions de votre cooperation
50, Avenue Pierre Mendes France - 75201 Paris cedex 13
Banques Populaires
Cas_3565851.zip

Ce message présenté comme provenant d'une banque comporte une pièce jointe apparemment dans un format de fichier compressé.

C'est une certaine forme d'ingénierie sociale car cela va inciter le curieux et l'indiscret à cliquer ouvrir la pièce jointe.

Le mal est fait.

Si vous avez de la chance, ce sera un simple petit virus que votre antivirus saura stopper, si toutefois vous en êtes équipés.

Dans le cas contraire, le risque peut aller jusqu'au chiffrement complet de vos données, lecteurs réseaux compris, Cloud compris.

Vos données seront alors inutilisables et vous verrez un message apparaître vous demandant d'envoyer une certaine somme sur un certain compte pour récupérer la clé de chiffrement qui devrait vous permettre de débloquer vos données.

Ce procédé est appelé en anglais le Ransomware traduit en français par le mot–valise de rançongiciel.

Si cela vous arrive, il est inutile de vous donner du mal à envoyer de l'argent, personne ne vous enverra jamais la clé de chiffrement. Réinstallez votre machine, munissez-vous d'un bon antivirus ou utilisez un système moins sensibles aux logiciels malveillants. (En d'autres termes, evitez Windows, le système pour lequel il existe le plus de "logiciels malveillants" en circulation).

2.5.2 Type de pièces jointes

Si vous avez le moindre doute, faites examiner votre ordinateur par un professionnel en lui expliquant ce qui vous est arrivé car il existe différentes menaces qui ne seront pas forcément facile à détecter par un antivirus.

- Les ransomware ou rançongiciels, leur fonctionnement est expliqué plus haut.
- Les Keyloggers : Ils vont intercepter vos mots de passe et permettre au pirate d'accéder aux sites auxquels vous accédez régulièrement,
- Les botnets : Ce sont des logiciels qui transforment votre PC en passerelle d'envoi de messages, utilisée pour le spam ou pour d'autres activités criminelles,
- les virus : ils vont affecter les performances de votre PC et peuvent détruire une partie de vos données ou de votre système d'exploitation après s'être automatiquement envoyé à tous les contacts de votre carnet d'adresses,
- Les vers qui se transmettent facilement d'un site Internet à votre PC puis de votre PC au site Internet suivant, sans que cela soit repérable.

– etc.

2.5.3 Avertissement relatif aux pièces jointes suspectes et malware

Si vous recevez un message de ce type, soyez très méfiant. Si vous n'avez pas de compte dans cette banque, détruisez le message, il est inutile de répondre au message car la plupart du temps l'adresse apparaissant comme celle de l'expéditeur n'existe pas. Le protocole de communication servant à l'envoi de courriels peut permettre facilement ce genre de manipulation.

2.6 Analyse de divers documents relatifs aux chaînes

Une chaîne peut paraître totalement anodine. On peut se dire que cela ne dérange personne que l'on fasse suivre. Détrompez–vous. Les chaînes sont des fléaux.

Pourquoi il ne faut jamais donner suite à ce genre de message et pourquoi il faut dissuader votre entourage de donner suite.

Gloablement le spam est un courrier indésirable ou pourriel (office québecois de la langue française)

Comme nous l'avons vu, les chaînes sont une de ses variantes.

Petit rappel prélevé dans le document général sur le spam :

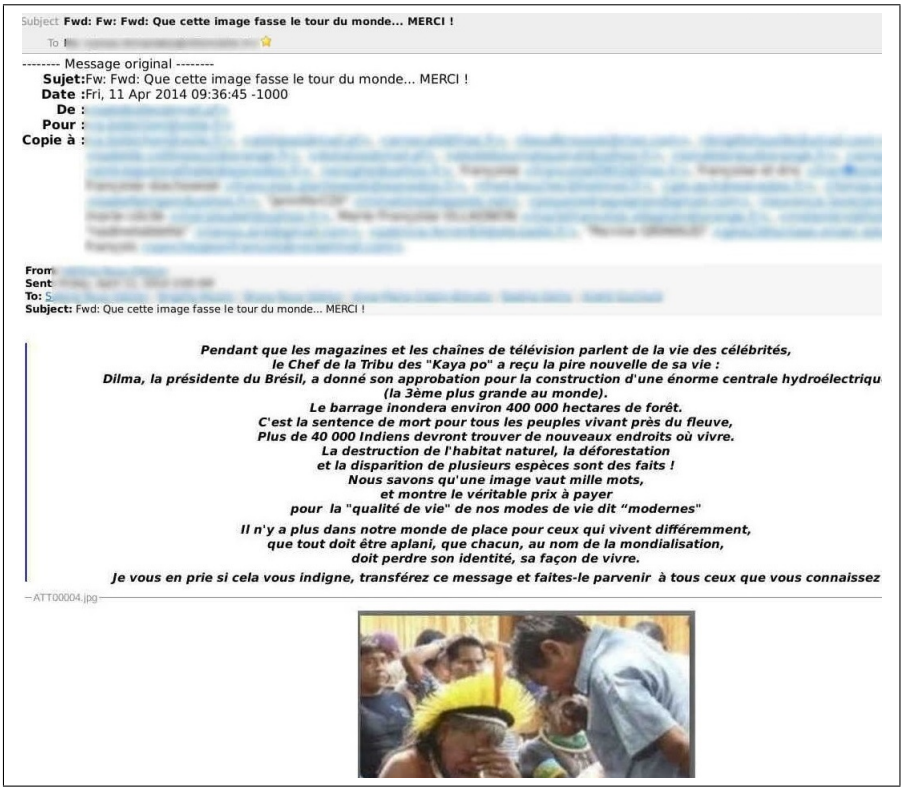
Il existe plusieurs catégories de chaînes :

- Des messages de chaînes colportant des nouvelles parfois totalement fausses ou proposant de remplir une pétition.
- Des messages indiquant qu'un virus existe et qu'on risque de recevoir un message avec ce virus, etc... c'est ce qu'on appelle un hoax (ou canular en bon français) Dites–vous bien que lorsque vous recevrez un virus, personne ne vous aura prévenu par mail.
- Chaînes de superstition.

Pour identifier facilement ce qu'est une chaîne et comprendre son fonctionnement, il est intéressant d'en avoir analysé une.

2.6.1 Un bel exemple de chaîne ci-dessous.

Cette chaîne transmise par vos amis l'a été pour une bonne raison, mais malheureusement cette transmission est totalement contreproductive et aura même un impact négatif.


Subject **Fwd: Fw: Fwd: Que cette image fasse le tour du monde... MERCI !**

To [redacted]

-------- Message original --------
Sujet: Fw: Fwd: Que cette image fasse le tour du monde... MERCI !
Date : Fri, 11 Apr 2014 09:36:45 -1000
De : [redacted]
Pour : [redacted]
Copie à : [redacted]

From: [redacted]
Sent: [redacted]
To: [redacted]
Subject: Fwd: Que cette image fasse le tour du monde... MERCI !

Pendant que les magazines et les chaînes de télévision parlent de la vie des célébrités,
le Chef de la Tribu des "Kaya po" a reçu la pire nouvelle de sa vie :
Dilma, la présidente du Brésil, a donné son approbation pour la construction d'une énorme centrale hydroélectriqu
(la 3ème plus grande au monde).
Le barrage inondera environ 400 000 hectares de forêt.
C'est la sentence de mort pour tous les peuples vivant près du fleuve,
Plus de 40 000 Indiens devront trouver de nouveaux endroits où vivre.
La destruction de l'habitat naturel, la déforestation
et la disparition de plusieurs espèces sont des faits !
Nous savons qu'une image vaut mille mots,
et montre le véritable prix à payer
pour la "qualité de vie" de nos modes de vie dit "modernes"

Il n'y a plus dans notre monde de place pour ceux qui vivent différemment,
que tout doit être aplani, que chacun, au nom de la mondialisation,
doit perdre son identité, sa façon de vivre.

Je vous en prie si cela vous indigne, transférez ce message et faites-le parvenir à tous ceux que vous connaissez

ATT00004.jpg

Un exemple de chaîne, totalement contre productif. Si vous voulez aider le chef Raoni, il ne sert à rien de faire circuler ce message pour vous donner bonne conscience. Cherchez plutôt une pétition sécurisée à signer, par exemple...

Dans ce message, j'ai compté 37 adresses électroniques visibles, parfois il y en a beaucoup plus.

Une aubaine pour les spammeurs toujours à la recherche de listes d'adresse mises à jour.

Cette chaîne manipule le lecteur en jouant sur les sentiments. Qui aime voir un vieillard pleurer ?

Qui a envie de se sentir responsable de la tristesse du chef Raoni que presque tout le monde connaît ?

Ce document est bien de l'ingénierie sociale, il incite le lecteur à faire suivre le message, sans réfléchir, mais justement, réfléchissons un peu ensemble :

- À quoi sert de faire suivre ce message à notre entourage ?
- À rien. Réfléchissez quelques secondes ? C'est sans appel ! Vous ne trouvez pas.
- En réalité, cela sert à obtenir des listes d'adresses car lorsque ces chaînes sont interceptées, il n'est pas rare de récupérer une centaine d'adresses et parfois beaucoup plus.

C'est triste à dire, mais les chaînes ne servent qu'à se donner bonne conscience lorsqu'elles portent les faux habits d'une noble cause.

Elles peuvent être une catastrophe lorsqu'elles font une dénonciation calomnieuse, c'est arrivé souvent.

Elles sont catastrophiques lorsqu'elles se mêlent de la vie privée.

Parfois, les chaînes utilisent la superstition. J'avais prévu un exemple de mon cru, mais finalement, j'ai choisi de présenter un message ironique trouvé sur Internet en cherchant des documents sur le sujet. Il est présenté à la fin de ce document.

2.6.2 Avertissement sur les chaînes

Si vous recevez un message de ce type vous intimant l'ordre ou vous demandant poliment de le faire suivre, il n'y a qu'une seule conduite à tenir : détruisez-le.

Contrairement à ce qui est écrit dans le message reçu, le monde ne se portera pas plus mal si vous arrêtez la chaîne. La transmission d'un message sur Internet contribue à la consommation d'énergie, or dépenser l'énergie est certainement le pire moyen d'aider le chef Raoni (Décidément, le choix de mon exemple était excellent).

Dans le cas des recherches de personnes disparues, l'inutilité de ce procédé n'est plus à démontrer, mais si vous avez encore un doute, je vous suggère cette lecture :

`http://www.hoaxbuster.com/hoaxliste/porte-disparu`

Concernant les recherches d'enfants disparus et les effets pervers que cela peut avoir, outre l'inefficacité, je vous invite à vous rendre sur cet autre lien :

`http://www.hoaxbuster.com/hoaxliste/enlevement-d-une-fillette`

Et plus globalement, hoaxbuster fait parti des sites que je recommande chaudement.

Toutes les techniques sont bonnes pour inciter à la précipitation. Ainsi, par exemple, certaines chaînes ou certains messages apparentés à des chaînes sur les réseaux sociaux vont commencer par des mots alarmistes tels que "ALERTE ENLÈVEMENT" par exemple.

Il est simple de prendre le temps de vérifier et quand bien même les informations s'avéreraient vrais, les médias font suffisamment de bruit dans ce cas. Les chaînes étant totalement inefficace et pouvant avoir des effets pervers, si vous devez faire circuler l'information, choisissez une forme classique.

Et pour finir, je ne résiste pas à la tentation de vous présenter une chaîne ironique, trouvée sur Internet alors que je cherchais des exemples à intégrer à ce document. (Bien que le chef Raoni n'y soit pas cité)

Je voudrais remercier tout ceux qui m'ont envoyé des e-mails en chaînes pendant toute cette année, car grâce à votre bonté:

1-J'ai lu 170 fois que MSN Hotmail allait supprimer mon compte

2-J'ai accumulé environ 3000 ans de malheur et je suis mort 67 fois à cause de toutes les chaînes que je n'ai pas renvoyées!

3-Quand je sors en boîte, je ne regarde personne, car j'ai peur qu'il (ou elle) m'emmène dans un hotel, qu'il (ou elle) me drogue, pour après m'enlever un rein pour le revendre au marché noir!

4-J'ai versé aussi toutes mes économies sur le compte d'Amy BRUCE, une pauvre petite fille qui était malade à l'hôpital plus de 7 000 fois (c'est drôle, cette petite fille a toujours 8 ans depuis 1995...)

5-Mon GSM Nokia gratuit n'est jamais arrivé, ni les entrées que j'avais gagnées pour les vacances payées à Disneyland.

6-J'ai inscrit mon prénom parmi 3000 autres sur une pétition et j'ai peut-être sauvé une espèce menacée d'écureuil nain à poil dur en biélorussie orientale .

7-Je connais la recette pour ne plus être seul en amour: il suffit d'écrire le prénom d'une personne sur un papier en pensant très fort à elle puis de se gratter (...) en tournant dans le sens des aiguilles d'une montre autour d'une Renault 4L (pas facile de trouver une 4L)

8-J'ai lu au moins 25 tomes de tous les préceptes du DALAI LAMA et j'ai accumulé du bonheur pour au moins les 4690 prochaines années!!

9-Sans oublier les 50 fois ou j'ai dû scruter mon écran nuit et jour pour détecter le fameux message qui contenait cet enfoiré de virus que même Microsoft, Mac affee, Norton Symantec etc étaient incapables d'avoir l'antidote et qui, non content de bousiller le disque dur, risquait de flinguer la chaîne stéréo, la télé, la cafetière et même le Sanibroyeur~!

IMPORTANT: si tu n'envoies pas cet e-mail dans les prochaines 10 secondes à au moins 8500 personnes, un dinosaure venu de l'espace viendra bouffer toute ta famille demain à 17h 30"

2.7 Cas particulier des attaques par téléphone

Il est apparu récemment un nouveau type d'attaque, très insidieuse réalisée par téléphone. Quelqu'un se présentant comme travaillant pour un éditeur de logiciel appelle pour signaler que votre machine a un problème que vous devez télécharger un petit programme afin de lui permettre de se connecter.

Une fois le petit logiciel installé par vos soins à la demande de l'interlocuteur, votre PC sera probablement intégralement chiffré et vous ne pourrez plus accéder à rien.

Si vous avez ce genre d'appel, ne faites rien de ce qui vous est demandé et si jamais vous avez laissé le pirate bloquer votre machine, refusez tout paiement en échange de déblocage car il ne débloquera rien.

Ne donnez jamais vos coordonnées car le pirate ne débloquera pas votre machine, mais en plus il utilisera vos informations bancaires à d'autres fins.

Allez porter plainte et adressez-vous à un vrai professionnel de

l'informatique pour réparer votre machine.

Aucun éditeur ne vous appellera si votre système n'est pas à jour, ou bien dans le cas contraire, vous aurez clairement la possibilité d'identifier la personne qui vous appelle mais ce genre de situation est extrêmement rare et se fait dans des cas d'infections massives avec le concours de votre fournisseur d'accès à Internet que vous pourrez clairement identifier.

Dans d'autres cas, ce sont des entreprises qui sont visées, ainsi un comptable sera appelé par son patron qui lui demandera d'effectuer de toute urgence un virement vers un compte dont il donnera les coordonnées.

Sauf que la personne qui appelle connait bien la société, mais n'est pas le patron et le compte bancaire de destination est situé dans un endroit échappant à tout contrôle.

Une fois le virement effectué, il ne reste plus qu'à virer l'employé qui s'est fait berner.

3 La propagation des malwares

La propagation des malwares se fait d'autant plus facilement que les antivirus ne sont pas à jour ou que les failles de sécurité des systèmes ne sont pas corrigées par des mises à jour. Tous les éditeurs, y compris ceux de logiciels libres, ont mis en place des systèmes de mises à jour plus ou moins automatique. A vous de régler les mises à jour comme vous l'entendez. Tous les systèmes ont des failles de sécurité, seulement certains sont beaucoup plus sensible que d'autres. ("Suivez mon regard", dit-il en regardant la fenêtre.)

3.1 Prévenir

Comment se prémunir d'une infection virale sur votre machine ?

Faites vos mises à jour de logiciels et de système d'exploitation régulièrement.

Ayez un antivirus en cours de validité et à jour.

Prenez toujours le temps de la réflexion avant de cliquer sur n'importe quel lien ou avant d'ouvrir n'importe quel fichier.

D'ailleurs, n'ouvrez jamais n'importe quel lien ou n'importe quel fichier.

Regardez l'exemple de la pièce jointe infectée située plus haut dans le document.

Si j'avais été un utilisateur de Windows, que ce serait-il passé ? Même avec un antivirus à jour, il n'aurait pas été totalement impossible que je subisse une infection.

De la même façon, si vous trouvez une clé USB par terre, et que vous la ramassez, ce doit être pour la recycler proprement dans un organisme spécialisé dans le traitement des déchets électroniques (DEEE) et certainement pas pour regarder son contenu.

Si on vous donne une clé USB, méfiez-vous, considérez toute clés USB comme une porte d'entrée potentielle pour une infection virale.

Le fait d'avoir un système à jour, un bon antivirus et un pare-feu à jour va vous protéger, mais les pirates ont souvent quelques longueurs d'avance.

Je n'utilise ni Windows, ni Mac OS X, mais je me méfie tout de même.

Il y a plusieurs types de malware de plus en plus complexes.

Certains se contentent de capter vos mots de passe, ce qui peut être gênant pour vos comptes bancaires. C'est d'ailleurs pour cela que la plupart des banques utilisent un clavier virtuel aléatoire pour les authentification.

Mais tout vos mots de passe peuvent être récupérés par ces logiciels qu'on appelle des "Keylogger", pas seulement ceux de votre banque.

J'ai déjà évoqué les ransomware, et il y a beaucoup d'autres périls. Vous allez me trouver alarmiste mais je veux simplement vous recommander la vigilance. Sortez de chez vous, mais regardez toujours à droite et à gauche avant de traverser la rue.

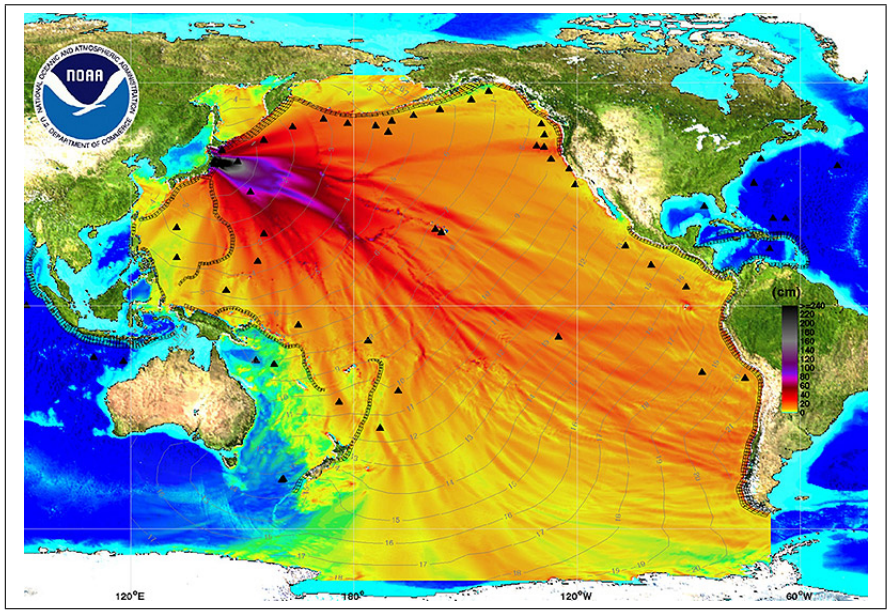
4 Manipulations sur les réseaux sociaux

La messagerie et Internet en général sont d'excellents outils pour apprendre, enrichir des compétences, partager des informations.

Mais ce sont aussi des outils de manipulation de masse qui, bien utilisés, peuvent provoquer des sortes de mouvement de foule virtuels.

Ainsi, une fausse information diffusée sur un réseau et propagée efficacement peut avoir des conséquences désastreuses.

Il s'agit parfois de désinformation, en manipulant une carte dont on donnera sciemment une interprétation et une légende fausses, par exemple, comme dans l'exemple ci-dessous, largement diffusé sur un réseau social.



Cette image de la NOAA représente les pics d'amplitude et la propagation des vagues du Tsunami qui a touché le Japon le 11 mars 2011.

Certains ont présenté cette image comme figurant la diffusion de la radioactivité dans tous le pacifique, à la suite du même tsunami, ce qui est bien sûr faux puisque cela ne correspond pas du tout aux courants marins.

Dans certains pays, les mouvements de foule virtuels sont parfois devenus réels, provoquant la mort de personnes accusées à tort de crimes qu'elles n'avaient pas commis.

Pour propager une nouvelle efficacement, il faut qu'elle soit présentée de façon à ce que le lecteur ait un sentiment d'urgence et ne juge pas utile de vérifier l'information.

Sur Internet, comme devant une télévision ou n'importe quel autre média, il faut toujours prendre le temps de vérifier l'information lorsque c'est possible. Même des journalistes sensés avoir du sens critique, puisqu'ils sont formés dans ce sens, se font parfois avoir en diffusant des nouvelles sans les vérifier.

Je vous ai parlé des fausses "alertes enlèvement" dans le chapitre précédent, il s'en trouve aussi sur les réseaux sociaux. Ne les relayez pas, laisser les autorités compétentes faire ce travail qui est le leur. Elle le font très bien et vous risquez de les déranger.

- Le 2 janvier 2013, un compte présenté comme celui de John Le Carré, sur le réseau des gazouilleurs, annonçait le décès de J.K. Rowling, beaucoup de gens l'ont cru.
- Le 12 aout 2014 était annoncé le décès du président rwandais Paul Kagame. Quand on sait comment le Rwanda a été touché quelques

années plus tôt, on peut penser qu'on a échappé à un mauvais scenario.
– etc.

Il arrive que ces messages soient relayés par des journalistes ou des célébrités qui ne les ont pas vérifié et se font donc piéger. Soyez plus malins qu'eux.

5 Quelques rappels indispensables et en vrac

Un premier conseil : Méfiez-vous des gens qui ont l'air de bien s'y connaître et qui vont polluer votre machine. Si vous avez un problème informatique, faites appel à un informaticien, pas à un bricoleur qui croit s'y connaître. Ne faites pas confiance à quelqu'un qui vous appel au sujet d'un problème informatique dont vous ignoriez l'existence. Si vous recevez un appel de ce type, raccrochez et si vous avez un doute, allez voir un professionnel. Si les appels se reproduisent, signalez–le aux autorités.

– Lorsque vous envoyez des messages en nombre, mettez toutes les adresses en copie cachée ou BCC pour "Blind Carbon Copy", certains logiciels utilisent l'abréviation CCi ou CCC.
– ne faites jamais suivre de chaîne, réfléchissez toujours avant d'exécuter une consigne, même si le motif ou la cause semble juste car il y a toujours des moyens plus efficaces d'aider le chef Raoni (en allant signer une pétition sur des sites spécialisés par exemple).
– Une chaîne va avoir un impact négatif sur votre niveau de crédibilité,
– Elle va étaler sur la place publique votre propre crédulité qui peut être accentuée par la fatigue, tout simplement, mais le mal est fait, (On ne vous cherchera pas d'excuse)
– Vous allez augmenter de façon drastique le nombre des spams reçus par vous et ceux dont les adresses apparaissent dans le message (avec les risques que cela comporte, si vous avez tout lu). Ils ne vous remercient pas.
– Cela va décrédibiliser certaines causes qui, bien qu'étant juste, se trouvent associées à ce mode opératoire stupide. (Le chef Raoni est un excellent exemple.)
– Votre banque ne vous enverra jamais de messages vous demandant des informations qu'elle est sensée déjà avoir.
– Si vous recevez un message provenant d'une autorité sensée avoir déjà vos coordonnées bancaires ou susceptible de vous demander de régler une facture, ou sensée avoir votre adresse de courrier

électronique et votre mot de passe, dîtes vous bien que ce message est certainement un faux.
- Les marabouts connaissent aussi les ficelles d'Internet, ne sous–estimez jamais les capacités de nuisances des spammeurs et ne répondez jamais à leur message, même si vous êtes excédés.
- N'ouvrez jamais les pièces jointes si le message vous semble étrange, si vous ignorez de quoi il s'agit ou si le message ne vous est pas destiné,
- Signalez les spam à l'organisme signal-spam. (voir ci-dessous)
- Si vous recevez un message vous indiquant que vous avez gagné ou que l'on a besoin de vous pour récupérer un héritage ou une grosse d'argent quelconque, ou encore qu'un inconnu, en train de mourir dans un hôpital avec un cancer du cerveau en phase terminale veut vous aider, détruisez ce message et faites savoir à votre entourage qu'ils doivent faire de même.

De toute façon, si vous avez un doute, mettez le message à la poubelle.

Récemment, il paraît qu'un professeur de philosophie de l'entourage de certains amis s'est fait avoir par une attaque d'hameçonnage et a communiqué son adresse courriel et son mot de passe sur un faux site qui ressemblait au site de messagerie utilisé habituellement.

Ensuite, l'escroc a fait de l'usurpation d'identité et a envoyé des vrais messages contenant de fausses nouvelles à tout le carnet d'adresse de ce monsieur. Le problème est que le pirate a eu accès aux messages de ce monsieur et a appris beaucoup de choses sur lui, y compris certaines de ses convictions qu'il souhaitait ne pas voir divulguées. Ce peut être très grave.

Si vous avez été victime de hameçonnage, il vous faudra porter plainte. Si l'escroquerie concerne vos informations bancaires, faites rapidement un signalement à votre banque.

Jusqu'à maintenant je pensais qu'avec un peu de sens critique on pouvait s'en prémunir. Le fait qu'un professeur de philosophie se soit fait avoir m'a inciter à revoir ma position et à rédiger cette série de documents.

5.1 Quelques sites de référence en matière de cybersécurité

Grâce aux derniers gouvernement, qui ont pris des décisions importantes dans ce domaine depuis 2012, la France est en train de rattraper en partie son retard en matière de cybersécurité.

Mais il y avait énormément de travail en la matière.

Et comme Internet n'est pas qu'un ennemi, voici quelques sites.

Le portail de l'Agence Nationale de la Sécurité des Systèmes d'Information :

`http://www.ssi.gouv.fr/`

Je vous le recommande car il contient énormément de renseignements et depuis peu les moyens de l'agence ont considérablement gonflé. Profitez-en, ce sont nos impôts et ils servent à quelque chose de vraiment utile.

Signaler un site Internet relatif à une escroquerie, un trafic, la pédophilie, etc.

`https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action`

Un site très ancien et toujours à jour répertoriant les canulars sur Internet. Il doit y avoir environ 15 ans que le site existe.

`http://www.hoaxbuster.com/` contre les canulars, excellent site en Français

La définition d'une chaîne de lettre sur Internet avec un historique et une analyse très intéressants :

`http://fr.wikipedia.org/wiki/Cha%C3%AEne_de_lettres`

Divers sites contre les escroqueries dîtes à la nigériane. (les scams)

`http://www.anti-scam.org/` (Site en anglais)

`http://www.419eater.com/` (Site en anglais)

`http://www.scamwarners.com/`

`http://www.antifraudcentre-centreantifraude.ca/` Site canadien bilingue.

6 En savoir plus sur la sécurité informatique

Cette partie arrive en fin de document car devant l'urgence de la situation, j'ai décidé de terminer par les généralités et de mettre en avant l'ingénierie sociale. Ce n'est pas l'ordre dans lequel j'avais prévu d'écrire ce document, mais devant la recrudescence des victimes, j'ai décidé de revoir ma copie.

La sécurité informatique est un vaste sujet qu'il faut prendre avec un peu recul afin de bien décomposer cette problématique.

On distingue 4 axes de travail que j'aurais aimé aborder. Cela fera l'objet de documents ultérieurs.

- L'approvisionnement énergétique,
- La sécurisation de l'accès physique aux machines,
- Les sauvegardes et tout ce qui en découle (Plan de reprise d'activité compris),
- La cybersécurité à proprement parler.

Chacun de ces axes peut être exploré avec un peu de sens critique et de logique grâce à un minimum de vulgarisation mais également un minimum de pages.

6.1 La cybersécurité

Il faut rester conscient que la cybersécurité ne s'arrête pas à l'étude de l'ingénierie sociale.

La racine cyber provient d'un mot grec signifiant pilote. Celui qui pilote est celui qui dirige un bateau par exemple, mais dans un sens imagé on peut y voir et on doit y voir le sens de gouvernant.

La cybersécurité est donc un très vaste sujet qui va de la prévention du piratage informatique en mettant en place des solutions matérielles ou logicielles pour s'en prémunir, à la recherche des solutions de sécurité et leur test, c'est ce qu'on appelle le hacking.

Le hacking consiste à chercher, à tester et parfois à pousser les sécurités dans leur dernier retranchement afin de mieux connaître leur limite.

Contrairement aux journalistes qui ont tendance à parler en experts de ce qu'ils n'ont pas forcément bien compris, je vais faire une distinction entre hackers et pirates. Les moyens mis en œuvre par les pirates ou les hackers sont les mêmes car pour tester la sécurité d'un produit ou d'un code, il faut tenter de les casser, mais leur objectif est différent.

Comme on l'a vu avec T.O.R. un outil destiné à améliorer la sécurité et la démocratie peut être détourné par des cybercriminels.

T.O.R. est un logiciel libre, développé par des hackers mais malheureusement très utilisé par des pirates.

Il existe différentes sortes de pirates :

1. Ceux qui travaillent pour une organisation criminelle (Mouvements intégristes, mafia, etc.),
2. Ceux qui travaillent pour le compte d'un état,
3. Ceux qui veulent juste se faire un nom et se faire reconnaître mais qui ont parfois un gros potentiel gaspillé,
4. Ceux qui ont téléchargé des modes d'emploi à l'usage du jeune imbécile qui veut faire croire qu'il est un vrai pirate, alors qu'il sait à peine lire un mode d'emploi,
5. Ceux qui sont intelligents mais ont peu de notions techniques. Ils ont une capacité de nuisance énorme et sont souvent dans les deux premières catégories. Bien qu'ils aient souvent assez peu de connaissances techniques, voire parfois pas du tout, ce sont les pires.

Pirater n'est pas seulement se connecter à un système informatique donné.

C'est aussi manipuler des machines ou des programmes informatiques, mais il est aussi possible de manipuler des humains, parfois simplement un peu fatigués ou dans une situation de détresse et pour cela il existe un certain nombre de techniques que l'on appelle "ingénierie sociale" et c'est ce que nous venons de voir dans les sections précédentes.

Ces techniques font plus appel à de la psychologie, parfois empirique, qu'à de la technique.

7 Le dernier mot de l'auteur

À travers ces quelques conseils, j'aimerai simplement que le grand public et en particulier les personnes peu habituées à l'utilisation d'ordinateurs se rendent compte que la sécurité informatique consiste d'abord à ne jamais se précipiter.

Travaillant dans l'informatique depuis plus de 25 ans, j'ai occupé divers postes. Mon expérience me donne un point de vue relativement large de plusieurs métiers de cette branche. J'ai été en contact avec mon premier virus informatique et mon premier "hoax" dans les années 1990.

Ayant administré des serveurs de messagerie et de partage ainsi que des parcs informatiques pendant bon nombre d'années, j'ai eu maintes fois l'occasion d'être au contact direct avec des utilisateurs parfois confrontés à ce problème.

La plupart des cas présentés ici sont récents, le plus ancien date de 2011.

Quelques deux illustrations de décoration présentes dans ce document sont des "open cliparts", elles sont donc libres de droits et sont accessible sur le site `http://openclipart.org/`.

Les autres images sont toutes des copies d'écran établies à partir de messages réellement reçus ou de vrais–faux sites Internet.

J.V. FERNANDEZ

Téléchargez une version ce document ou mon CV grâce aux qrcodes :

Document à jour

Mon CV à jour